Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 129 (2018) 324–330

Procedia
Computer Science

www.elsevier.com/locate/procedia

2017 International Conference on Identification, Information and Knowledge in the Internet of Things

Mobile Network Security and Privacy in WSN

Yuan Gao[a,b,c,d,*], Hong Ao[b], Zenghui Feng[b], Weigui Zhou[b], Su Hu[c], Wanbin Tang[c]

[a]*Academy of Military Science of PLA, Beijing, 100030, China*
[b]*Xichang Satellite Launch Center, Xichang, 615000, China*
[c] *University of Electronic Science and Technology of China, Chengdu, 610054, China*
[d]*State Key Laboratory on Microwave and Digital Communications, National Laboratory for Information Science and Technology, Tsinghua University, Beijing, 100084, China*

Abstract

This paper discuss the term threats, attacks and vulnerabilities in Wireless Sensor Networks followed by a model that relates the three entities. Based on the model, a framework of Trusted Wireless Sensor node is presented consisting of two major sections which are platform security enhancement and Trusted Authentication protocol to enhance sensor nodes security features and confirm the fidelity of node joining the network respectively. The design of the framework is in line with Trusted Computing Group specifications toward trusted platform implementation. Finally, brief analysis on the proposed framework is presented.

Keywords: Wireless Sensor Network, security, threats, attacks, vulnerabilities, Trusted Computing

1. Introduction

Wireless Sensor Networks (WSNs) is network consisting of thousand sensor nodes or motes communicating wirelessly with each other and with base station. While sensor nodes perform specific task at the intended location, base station which is a more powerful device, act as a front-end to WSNs users hence offering the functionality of sensory systems to computer systems. Further, the benefits of using WSNs technology also is undeniable including easy and inexpensive deployment due to the use of wireless interface, running unintendedly or less supervision and longer surviving time in its deployment area.

The range of potential applications that WSNs may offer is immeasurable by reason of unlimited imagination and is currently ranging from basic temperature measurement to complex applications. Such applications include personal sensing [1], body area network [2, 3], military [4], smart building [5] and camera and video surveillance

10.1016/j.procs.2018.03.083

[6] . It is believed that, advancement in sensor technology, low power embedded processor, wireless communication technology and the network technology greatly contributed to the establishment of tremendous WSNs applications in today's and future way of life.

However, security plays an important role in realizing those applications to reality. Security challenges in WSNs can be divided into three different categories that are related to each other. The first should be on securing the sensor node or the platform itself so the network originator can guarantee the integrity of the sensor or node exists in the network. This is followed by the big challenges faced in securing the network infrastructure or wireless medium to ensure reliable, secure and trusted communication. Finally, protecting the data (confidentiality and integrity) is also a challenge in wireless communication where anyone can intercept the data due to the nature of wireless communications.

The rest of the paper is organized as follows: Section 2 discusses the relationships between threats attacks and vulnerabilities in WSNs area. Section 3 briefly discusses the proposed security framework, followed by Section 4 which introduces the research tools. Section 5 presents the security analysis of the proposed protocol and brief significant contribution is presented in Section 6. Finally the conclusion is addressed in Section 7.

2. Threats, Vulnerabilities and Attacks in WSNs

Threats, vulnerabilities and attacks are three crossly related entities that usually caused havoc in the security field.

Subsequent paragraph briefly discuss each term and conclude with a model to show the relationship between the three entities.

2.1. Threats

Threat is defined as the ability or intention of any agent to adversely affect the operation, system or facility offered by that network. It can be categorized into amateur, professional and well-funded adversary. Amateur types of attacks include denial-of-services or eavesdropping through wireless sniffing. A professional type of adversary usually launches more sophisticated attacks such as hijacking, man-in-the middle or Sybil attack. Finally a well-funded adversary with highly sophisticated tools will launch attacks such as node capture, wormhole or rushing attacks [7].

2.2. Vulnerabilities

Anything that leaves an information system open for potential exploitation is called vulnerabilities. The nature of WSNs itself such as physical limitation and network constraint can be said as major sources of vulnerabilities to WSNs applications. These include: 1)Wireless link that is open to everybody to intercept or unstable link that lead to nodes uncertainty thus difficult for TMS or intrusion detection system (IDS) to detect malicious node.2) Limited energy – nodes may disappear anytime or adversary may launch DDoS attacks to exhaust the battery of a legitimate node. Beside nodes near to BS also deplete faster compared to other nodes in the networks [8]. 3) Unattended node – vulnerable to being physically captured and results to exposure of cryptographic keys. 4) Multi-hop communication – needs high cooperation from intermediate nodes. Malicious nodes may refuse to forward the packet, drop or even modify the data. 5) Limited computational ability especially for sensor node with low processor bits and frequencies and smaller memory sizes. 6) Existing vulnerabilities in wired link such as DDoS, spoofing, passive eavesdropping and many more [7].

2.3. Attacks

Attack is an action with an intention to bypass security control on a system. It can be classified as passive, active and physical types of attacks and can be performed by insiders or outsiders.

1) Passive attacks: The adversary's goal is to obtain important information quietly and unnoticeable by anyone. The collected data from single or many nodes for certain period of time will be analyzed to launch new active attacks or to extract secret information from the packets. Some of the possible types of passive attacks are eavesdropping and traffic analysis. 2) Active Attacks: The attackers or adversaries usually exploit the security holes in the networks to launch attacks such as packet modification, injection or replaying. These include sleep deprivation, replay and DDoS attacks. Latest, over-the-air programming has been employed for remote software update. Although it has been found useful for researchers and network owners, the procedure generally leaves the door "wide open" for injection of malicious code. Even though it is hardly done, Francillon[9] in his work has successfully injected malicious code in Micaz class motes thus triggering the alarm for holistic security in wireless sensor network. 3) Physical attacks: Physical attacks refer to attacks that involve direct connection with the sensor node. Roosta et al. in [10] have divided physical attacks into two classes; invasive and noninvasive. While invasive require sophisticated tools on the site or away from the site, the non-invasive is much easier and usually attacked through JTAG port that is widely used during the development and debugging phase. By enabling JTAG port, adversaries will have the capability to take control of the whole system. Invasive attack is possible through the physical capture of a sensor node. As of yet, there is no solution available to make the sensor nodes resistant to physical tampering; as listed in Table 1 the sensor nodes' micro-controllers lack any kind of hardware-based memory protection and mostly not designed with security features.

In embedded systems, crypto-processors or physically secure processors have been used extensively to provide some level of resistance to physical tampering. Even though attacks on crypto-processors are known to occur, they still provide a first line of defense against physical tampering. Therefore, optimizing crypto-processors to fit the low-cost, low-energy requirements of sensor networks can play a significant part in raising the level of security achieved. Non-invasive attacks, such as side-channel attacks, are also possible in sensor networks. For example, a study by [11] and [12] has shown that side-channel attacks can be launched using simple power analysis as well as differential power analysis in embedded appliances. Their results suggest that several key bits can be extracted through the power analysis attack.

Another form of attack is by exploiting the Bootstrap Loader (BSL) and this mostly happens during the boot up process. With having access to the boot devices and debug session, attackers will be able to study the systems and its operation thus providing them with enough information to clone the system, insert malware and disturb the overall operations of the sensor node and its systems [9-13]. Intention for physical types of attacks might vary from to destroy the sensor node, extracting private information and finally to being authenticated or being authorized in the network. Also, successful physical attacks will leads to node cloning attack where adversaries will introduce the network with one or many cloned nodes.

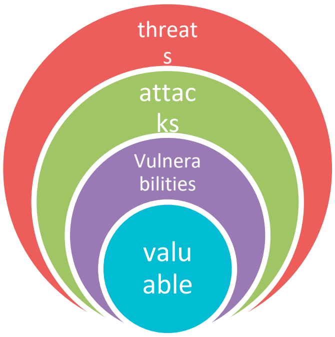

Fig. 1. Threats, attacks and vulnerabilities (TAV): Its relationship

Relationship between threats, vulnerabilities and attacks can be portrayed as in Fig. 1. Threats that come from various background and identities and with various difference intentions will generate various types of attacks to steal valuable information from the entities. Moreover, successful of attacks is very much depend on the vulnerabilities surrounding the valuable entity, referring to sensor node in this case. However, with difficulties to predict threats from adversaries together with existing vulnerabilities exist in the network due to the WSNs nature, this work decide to enhance the security features at the sensor node platform and provide a concrete method to prevent illegal nodes from joining the network.

3. Proposed Security Framework

Security in WSNs very much depends on the intended applications. Certain group of network might require high data security that includes secure transmission, secure storage and secure network management and also trusted node. A lot of studies have been done in this area that includes routing protocol, node authentication [14-16], key distribution [17] access control [18]. Unfortunately, these security design usually only covers attacks related to network and communication. Based on the TAV relationship, proposed works aimed at enhancing the security features of the valuable entities which is the sensor node in this case, to reduce the effect of node capture attack and to minimize the possibility of node being cloned in WSNs environment. Table 1 tabulated existing famous sensor node and its platform security features.

Proposed security framework is best classified into two parts which are enhancing the platform security features and registering valid nodes to the network. Both parts when combined produced a complete trusted platform according to Trusted Computing Group Specifications.

Table 1. Sensor Nodes and Security Features

Sensor Node	Processor	Security features
Crossbow Motes	Atmel 128 -8 bit $^{1\&2}$	Not mentioned^{1}
^{1}Mica2	Texas Instruments	AES128^{2} hardware
^{2}Micaz	MSP430 -16 bit ^{3}	Not Mentioned^{3}
^{3}TelosB		
Imote 2	Marvell PXA271 13-416 MHz - 32 bit	Not mentioned
Tmote-Sky	Texas Instruments MSP430 -16 bit	Not mentioned
SunSpot	ARM9(180MHz)-32 bit	Not mentioned
^{4}Csiro Fleck	ATMega128L (4/8MHz)	Not mentioned^{4}
^{5}TrustFleck	-8 bit	TPM chip^{5}
Proposed	ARM1176JZF-s 32-bits (667MHz)	Secure storage and dual operating mode

3.1. Platform Security Features

As mentioned earlier, sensor node are exposed to node captured attack that later exposed sensor node sensitive data and credentials to adversaries. To minimize the effect to this attack, the sensor node security features should be enhanced. Proposed sensor node platform supports this through:

1) Protected memory to securely kept sensor node private key and other sensitive credentials. 2) Trust Zone features that divide execution mode and memory region into secure and non-secure mode and region. 3) Secure boot process that measure the integrity of boot up images and selected peripheral on the sensor node platform and finally. 4) Sensor node unique identity that is generated based on selected components unique value on the platform.

3.2. Platform Security Features

To prevent unauthorized nodes in the network, proposed worked utilized node identity and node management value that were uniquely generated upon node first boot-up. The values together with identity based cryptography (IBC) algorithm were used in the authentication protocol named IBE-Trust.

Framework of the protocol is presented. IBE-Trust is provide a secure platform for valid nodes to report its management value to base station upon node first boot-up at the deployment location. With wireless as the medium of communications in WSNs environment, secure communication between nodes in the network is a necessity. Basic security features that IBE-Trust offered are:
1) Confidentiality: to confirm that the messages sent are unreadable to any unintended receiver including eavesdroppers. Established by encrypting the message with base station public key. 2) Authenticity: to confirm that the packets or messages received are from valid sender. Established by authenticating the sender identity. 3) Integrity: to confirm the genuineness of the packets received. Established through Message Authentication Code (MAC) algorithm.

Summarized process flow of the proposed framework is presented in Fig. 2. First stage happened at the sensor node with the intention of confirming the integrity of codes running. Outcome from a so-called measurement process is a unique value that represent platform unique entity. This stage also generate platform unique identity that will be used in the identity based cryptography protocol. Upon successful boot up, sensor node will report its measurement value to base station. The value is sent encrypted to base station (BS) using a developed protocol named as IBE-Trust protocol. This protocol will ensure message confidentiality, authenticity and integrity. Once BS received the value, authentication on sender unique identity will be done followed by verification on the measurement value to confirm the trustworthiness of node that joined the network.

4. Security Analysis

We briefly describe the selected hardware and software used in this research.

ARM11 Processor: The target processor used in this project is the ARM1176JZF-S with trust zone features that enhance security aspect through separation between normal and secure environment. Beside the processor is optimized for low power environments and employs RISC architecture that support constraint in WSNs.

ARM Real View Development Suite (RVDS): This software is used to load the developed codes into the ARM1176JZF-S development board.

MIRACL library: MIRACL is a C and C++ library for cryptographic code. Support Elliptic Curve Cryptography over $GF(p)$ and $GF(2^m)$, which is required for Tate Pairing algorithm that is used in IBE-Trust protocol.

AVISPA and SPAN is one of the model checking tool and utilized high-level formal language HLPSL for specifying protocols and their security properties. The developed model of the IBE-Trust protocol is converted to an intermediate format (IF) and fed to one of the four backbends named: SAT-based Model-Checking (SATMC), On-The-Fly-Model-Checker (OFMC), Constraint Logic Based (Cl-Atse) and TA4SP for verification. Each backbends basically used different technique but complement to each other.

Attestation: To further analyses the functionality of IBETrust protocol, an attestation consisting of two computers connected to ZigBee transceivers is set up in the laboratory.

Besides, the attestation allows further analysis on the protocol such as communication overhead to be done.

4.1. Physical attacks

Introducing the use of ARM1176JZF-S as the processor with its on-SoC memory has helped this study to protect important credentials such as sensor node private keys. In this scheme, only part of the private key is stored in the sensor node memory thus further protect the sensor nodes and network. Images such as encryption and decryption are stored in the secured memory region of flash memory and are only accessible in the secured mode environment. The effect of BSL attacks can also be reduced through the secure boot process where the integrity of images loaded has been verified to prevent sensor nodes from running malicious code.

4.2. Node impersonation

Node impersonation happens when intruders manage to duplicate the unique identity of the sensor node that is being used during authentication. Non-regeneration of the same trust value through secure boot process has significantly reduced the possibility of having a masquerade node in the network.

4.3. Typical wireless attacks

This study also confirms that the communication during trusted authentication is free from active attack such as message modification, replay attack, and false message through packet encryption, nonce value as well as entity and data authentication.

4.4. Security of the proposed scheme

The security of IBE-Trust protocol is best realized through the security of full BF IBE scheme. In this scheme, the public key can be written as $Q_{ID} = tP$ for some unknown t. Therefore $\hat{e}(rQ_{ID},sP) = \hat{e}(rtP,sP) = \hat{e}(P,P)^{rst}$ and cipher text $C = (rP, M \oplus H_2\hat{e}(P,P)^{rst})$. If an adversary manages to get P and sP from the public parameters, they can calculate $Q_{ID} = tP$ from receiver's identity and observes rP in the cipher text. Moreover, if the adversary manages to calculate $\hat{e}(P,P^{)rst}$ from P,sP,rP and tP then he will be able to recover the message M by calculating $(M \oplus H_2\hat{e}(P,P)^{rst} \oplus H_2\hat{e}(P,P)^{rst}))$ = M.

Calculating $\hat{e}(P,P)^{rst}$ is actually solving Bilinear Diffie-Hellman Problem (BDHP) and is very difficult. This brief analysis confirms the confidentiality of unique trust value of each sensor node in the network that is sent to BS encrypted with IBE scheme. For node to node authentication, our proposed scheme uses the ID-based one-pass AKE. In a previous existing protocol presented, the authentication is established when both parties manage to generate similar shared key locally. In our proposed protocol, beneficiary node will first check the identity of nodes requesting to authenticate and proceed to compute the secret shared key if the ID exists in the table provided by BS. This somehow has provided a two tier security mechanism and has limited this expensive operation to valid nodes only. Identity-based one-pass AKE is based on symmetric bilinear pairings and is secure by assuming the hardness of BDHP with H_1,H_2 and κ modeled as random oracle. Interested readers can find proof to this method.

Acknowledging the limited resources of widely used sensor node, the proposed scheme does not burden the sensor nodes with intensive computations such as key generation. Besides, proposed scheme enhances security level by introducing platform integrity measurement and reporting to ensure the integrity of codes running in the platform. Another, if a sensor being stolen, no private key can be regenerated as no master key is kept in the sensor node. Finally, the identity used in the IBC algorithm is uniquely generated based on platform components as contrast to widely used string based identity thus eliminate possibility of duplicate identity and cloned node in WSNs.

5. Conclusion

This paper presents the relationships between threats, attacks and vulnerabilities that exist in common WSNs environment. Outcome from the analysis is a model named TAV that shows the demand on enhancing the security features at the platform level of the sensor node. Summarization on the developed framework is presented focusing on the mechanism and steps involved to enhance sensor node security features. On the other hand, the framework is design based on the trusted platform specifications as outlined by TCG to provide a concrete way of conforming node trustworthiness in the network. To avoid node cloning which mostly happened as a result of node capture attack, a unique non-duplicate hash value is used instead of widely used string based identity. Finally, proposed framework is design with resource constraint in mind to confirm its functionality in WSNs environment.

Acknowledgements

This work is funded by National Natural Science Foundation of China (61701503).

References

[1]. Filippini, Massimo, and Lester C. Hunt. (2011) "Energy demand and energy efficiency in the OECD countries: a stochastic demand frontier approach." *Energy Journal* **32** (**2**): 59–80.

[2]. B. Mostefa and G. Abdelkader, "A survey of wireless sensor network security in the context of Internet of Things," 2017 4th International Conference on Information and Communication Technologies for Disaster Management (ICT-DM), Münster, Germany, 2017, pp. 1-8.

[3]. B. Doyle, S. Bell, A. F. Smeaton, K. McCusker and N. E. O'Connor, "Security Considerations and Key Negotiation Techniques for Power Constrained Sensor Networks," in The Computer Journal, vol. 49, no. 4, pp. 443-453, July 2006.

[4]. A. Praveena, "Achieving data security in wireless sensor networks using ultra encryption standard version — IV algorithm," 2017 International Conference on Innovations in Green Energy and Healthcare Technologies (IGEHT), Coimbatore, 2017, pp. 1-5.

[5]. A. Rani and S. Kumar, "A survey of security in wireless sensor networks," 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT), Ghaziabad, 2017, pp. 1-5.

[6]. S. Pourazarm and C. G. Cassandras, "Energy-Based Lifetime Maximization and Security of Wireless-Sensor Networks With General Nonideal Battery Models," in IEEE Transactions on Control of Network Systems, vol. 4, no. 2, pp. 323-335, June 2017.

[7]. Guyue Li and Aiqun Hu, "Virtual MIMO-based cooperative beamforming and jamming scheme for the clustered wireless sensor network security," 2016 2nd IEEE International Conference on Computer and Communications (ICCC), Chengdu, 2016, pp. 2246-2250.

[8]. N. Bisht, J. Thomas and V. Thanikaiselvan, "Implementation of security algorithm for wireless sensor networks over multimedia images," 2016 International Conference on Communication and Electronics Systems (ICCES), Coimbatore, 2016, pp. 1-6.

[9]. A. Bushang and A. Mahmood, "A specialized event-driven network simulator for security and anonymity applications of Wireless Sensor Networks," 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, 2017, pp. 1-6.

[10]. H. Fouchal, J. Biesa, E. Romero, A. Araujo and O. N. Taladrez, "A Security Scheme for Wireless Sensor Networks," 2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, 2016, pp. 1-5.

[11]. S. Anbuchelian, S. Lokesh and M. Baskaran, "Improving security in Wireless Sensor Network using trust and metaheuristic algorithms," 2016 3rd International Conference on Computer and Information Sciences (ICCOINS), Kuala Lumpur, 2016, pp. 233-241.

[12]. A. Praveena and S. Smys, "Efficient cryptographic approach for data security in wireless sensor networks using MES V-U," 2016 10th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, 2016, pp. 1-6.

[13]. Yang Xiaomei and Ma Ke, "Evolution of wireless sensor network security," 2016 World Automation Congress (WAC), Rio Grande, 2016, pp. 1-5.

[14]. B. D. Beheshti, "A framework for Wireless Sensor Network security," 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, 2016, pp. 1-4.

[15]. A. Chowdhury, F. A. Tanzila, S. Chowdhury and M. M. Haque, "An efficient security architecture for Wireless Sensor Networks using pseudo-inverse matrix," 2015 18th International Conference on Computer and Information Technology (ICCIT), Dhaka, 2015, pp. 396-400.

[16]. R. Fisher, M. Lyu, B. Cheng and G. Hancke, "Public key cryptography: Feasible for security in modern personal area sensor networks?," 2016 IEEE International Conference on Industrial Technology (ICIT), Taipei, 2016, pp. 2020-2025.

[17]. E. Brumancia and A. Sylvia, "A profile based scheme for security in clustered wireless sensor networks," 2015 International Conference on Communications and Signal Processing (ICCSP), Melmaruvathur, 2015, pp. 0823-0827.

[18]. Anita Daniel. D and Emalda Roslin. S, "A review on existing security frameworks with efficient energy preservation techniques in Wireless Sensor Networks," 2015 International Conference on Communications and Signal Processing (ICCSP), Melmaruvathur, 2015, pp. 0658-0662.