

A study on sensor nodes attestation protocol in a Wireless Sensor Network

Yong-Sik Choi*, Young-Jun Jeon*, Sang-Hyun Park*

* Dept. of Computer Science & Engineering, University of Incheon,
12-1 SongDo-Dong, Yeons-Gu, Incheon, South Korea

mars@incheon.ac.kr, 0961144@incheon.ac.kr, tank1862@nate.com

Abstract— A sensor network is applied to various fields from the special application fields such as wild environment monitoring, industrial machine measurement, and military-purpose measurement to the daily application fields such as fire monitoring and pollution monitoring. A Wireless Sensor Network is a wire and wireless network, which consists of several sensor nodes deployed in a certain field. A sensor node should have computation, sensing and wireless communication functions. A sensor network has a limited computing and communication resource. To overcome this barrier, collaboration with surrounding nodes is required. In other words, information sharing between hierarchies is required rather than a hierarchical approach. A sensor network generally consists of a large number of sensor nodes for exact sensing and extendibility of the sensing areas. Therefore, attackers can easily capture sensor nodes. And an attacker is able to attack the sensor node itself and the sensor network through a modified attack on sensor nodes. Therefore, the security of a sensor network is important. The attestation for sensor nodes suggested by this paper consists of 2 steps. STEP 1. Inter-connective attestation between surrounding sensor nodes STEP 2. If there is any abnormality, the node notifies the BS (Base Station) and requests attestation as to whether there is a damaged node or not. Initial sensor node attestation is carried out by inter-connective sensor nodes, not by the BS. If there is any abnormality, the node notifies the BS. And BS carries out attestation for node showing abnormality. Attestation for the BS and sensor node uses an authentication protocol method for preventing nodes from being captured. As mentioned above, because there is a periodic simple attestation procedure between sensor nodes and sensor node attestation, it is easy and rapid to identify which is captured by attacker; thus, a secure sensor network is attainable.

Keywords— Sensor node, attestation Wireless network

I. INTRODUCTION

Sensor networks are applied to various fields ranging from special application fields such as wild environment monitoring, industrial machine measurement and military-purpose measurement to daily application fields such as fire monitoring and pollution monitoring.

A wireless sensor network is a wire and wireless network, which consists of several sensor nodes deployed in a certain field. A sensor node should have computation, sensing and wireless communication functions.

A wireless sensor network limits the radio frequency channel, due to, that is to say, unstable links, limit of physical protection of each sensor node, actual of each nodes connection, variation topology in addition dangerousness about routing security is high by activity spite nodes. In addition, restrictions of the hardware of the sensor node itself makes it difficult guarantee the maintenance of security because of vulnerability [1], [2].

A sensor network has limited computing and communication resources. To overcome this barrier, collaboration with surrounding nodes is required. In other words, information sharing between hierarchies is required rather than a hierarchical approach. A sensor network generally consists of a large number of sensor nodes for exact sensing and extendibility of sensing areas. Therefore, attackers can easily capture sensor nodes. And the attacker is able to attack the sensor node itself and the sensor network through a modified attack on the sensor node. Therefore, the security of a sensor network is important. The attestation for sensor nodes suggested by this paper consists of 2 steps.

STEP 1. Inter-connective attestation between surrounding sensor nodes

STEP 2. If this is any abnormality, the node notifies the BS (Base Station) and requests attestation as to whether there is a damaged node or not. Initial sensor node attestation is carried out by inter-connective sensor nodes, not by the BS. If there is any abnormality, the node notifies the BS. And the BS carries out attestation for the node showing abnormality. Attestation for the BS and the sensor node uses the authentication protocol method for preventing nodes from being captured.

The composition of this paper is as follows: in the second section, attestation technologies and hardware-based and software-based sensor node security is discussed. In the third section, the sensor nodes attestation protocol in Wireless Sensor

Networks is discussed. The fourth section discusses security considerations. And the conclusion is in the final section.

II. RELATED WORK

Verification technology for attesting that codes running in each sensor node are not changed is generally used to solve program modification in sensor nodes. Programs by vicious attacks and unexpected error can be detected.

By attesting program memory in the memory node of the sensor node under which a modified program for vicious attacks is running, it is possible to detect the sensor node in which programs for vicious attacks and unexpected errors are running [3], [4].

1) Attestation is carried out with software and hardware methods.

2) Hardware attestation is carried out through equipment equipped with hardware developed by TCG (Trusted Computing Group), NGS (Nest-Generation Secure Computing Base), and software attestation is carried out by attesting memory area of sensor node through communication between the sensor nodes of the attester.

3) The SWATT (SoftWare-based ATTestation) method attests for targeted equipment and devices the challenge-response protocol.

A. Attestation technology

Attestation proves that modifications to the software or hardware in the targeted device have not been arbitrarily carried out by an attacker. In other words, attestation proves the integrity of the software or hardware for the targeted device.

B. Hardware-based attestation technology

TPM (Trusted Platform Module) is the hardware-based attestation specified by TCG (Trusted Computing Group), and uses smart cards as reliability devices to achieve reliability. TPM provides a protected storage area for an advanced hardware engine and an encryption key for creating an arbitrary number, key calculation and hash calculation. TPM is capable of creating and storing symmetric and asymmetric keys, and of executing asymmetrical encryption calculations. In addition, TPM provides PCRs (Platform Configuration Registers), which are used for storing platform-dependant set values. PCRs are initialized when power is given to them, and the software components (BIOS, boot loader, OS, applications) are evaluated as TPM before they are executed; the calculated hash value is stored in a specific PCR [4].

CRTM (Core Root of Trust Measurement) residing in the BIOS, which is first executed when power is given to it, evaluates itself and the BIOS and transfers control to the next software component.

All the evaluated components create an SML (Stored Measurement Log) and record the results. The PCR value can be used with SML together for remote equipment to attest the targeted equipment's status, and uses authorization through an AIK (Attestation Identity Key) that is impossible move in order to guarantee the exactness of the PCR value.

Remote equipment is able to prove the integrity of the targeted equipment through verification of authorization, and is able to compare the PCR value. TPM provides a sealing function by which a data block can be connected to a set value for a specific platform. A sealed message consists of range value for the platform-set registry, an unmovable key value, and a sealed data block.

If the sealed platform set value is equal to those in the current platform, then TPM performs decryption for the sealed message and transfers it. But the method using the TPM chip is not suitable for a sensor network that has low cost for each sensor node.

C. Software-based attestation technology

The software-based attestation methods include sharing basic threshold secrets, majority vote, and SWATT [5], [6].

Attestation methods based on sharing basic threshold secrets and majority vote store noise in the empty program memory area before laying sensor node, and they use block-based pseudo arbitrary memory search for calculating checksum. Noise creation encrypts count values starting at 0 as RC5 by using a unique seed value for each node.

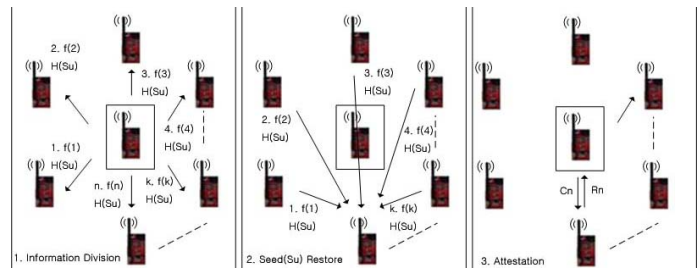


Figure 1. Attestation of basic secure public critical value

As shown in Figure 1, the method based on sharing basic threshold secrets consists of the following 3 steps.

STEP 1. A sensor node creates unique noise and stores it in the empty memory before the node is laid out. After the sensor nodes are laid out, and at least before sensor nodes are modified by an attacker, they find neighboring sensor nodes and create an arbitrary constant value less than the number of found sensor nodes and create a polynomial expression (1). After the sensor nodes calculate x , $f(x)$ from 1 to next to the node by using polynomial expression (1), and distributes it to neighbor sensor node with hashed S_u .

$$f(x) = S_u + a_1 x^1 + a_2 x^2 + \dots + a_{(k-1)} x^{(k-1)} \quad (1)$$

(S_u : noise generation seed, $1 \leq k \leq \text{neighbor node}$)

STEP 2. Based on the specific head selection algorithm, the header is chosen, and S_u is calculated by receiving k numbers among n number of $(x, f(x), H(S_u))$ which were previously laid out from the neighbor sensor node.

STEP 3. The header sends an arbitrary challenge value to the sensor node to be attested, and internally calculates the checksum of the targeted node through self-calculated S_u . If the checksum received from the sensor node to be finally attested is equal to that of the internally calculated checksum, the targeted node is proved to be a normal sensor node that has not been modified by an attacker. The attestation method based on

sharing a basic threshold value secret has a problem: the method cannot prove the exactness of the attestation if the node that is selected as cluster header is modified by an attacker. Therefore, a method based on the majority vote by neighbor nodes to be attested is developed instead of developing specific cluster header selection. This majority vote-based attestation method consists of 2 steps, as shown in Figure 2.

STEP 1. Before the sensor nodes are laid out, noise by unique seed and n number of pairs in challenge/response, which are expected for the layout, are calculated in advance and stored in the memory. And after the sensor node is laid out, one of n number of challenge/response is arbitrarily selected one by one, and sent to the found neighbor sensor node.

STEP 2. Neighbor sensor node that had received challenge/response, along with the challenge that was received for attesting the sensor node that has sent the challenge/response, sends a serial number to the corresponding sensor node to prevent attack by replay as RC5 by using a unique seed value for each node.

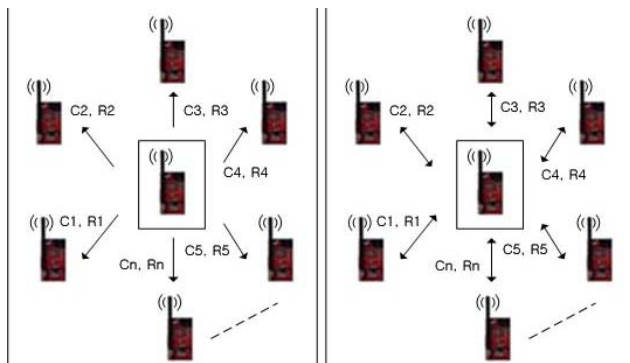


Figure 2. Attestation of majority-vote-based verification

The sensor node that received the challenge and the serial number sends a response by calculating the memory checksum. If more than half of the responses for the challenge sent by the neighbor sensor node are proved to be equal, then the corresponding node is proved to be a normal sensor node.

As the two methods described above use cooperation of several numbers of neighbor nodes to be attested, i.e., cooperation by neighbor nodes when sensor nodes are laid out, in other words, the nodes use a method for distributing data necessary for attestation to the neighbor node for the layout of the sensor node, they can't perform attestation if the neighbor node that has distributed data disappears.

Therefore, these two methods are not suitable for a sensor network that has a lot of variation in the network. Furthermore, these two methods require much memory space for storing distributed data when there are many neighbor nodes. Attestation based on majority vote has a problem which should many of neighbor nodes for attesting one sensor node. And it cannot identify a damaged node from attacking after performing attestation.

The SWATT (Software-based ATTestation) Method, differently from hardware-based attestation method, is a software-based technology for attestation that attests memory content (code, static, data, set value for devices) for embedded devices without hardware devices.

The SWATT method carries out attestation using the challenge-response protocol between embedded devices by laying remote attestation equipment. As the SWATT method isn't accompanied by additional hardware cost, this method is suitable for a sensor network environment with several hundreds and thousands of sensor nodes.

The attestation device in the SWATT method sends an arbitrary challenge to an unattested device. The device that received the challenge calculates the memory checksum, and then returns a response to the attested device. In this case, the attestation device has already known the value of the built-in memory in the device, so the attestation device internally calculates the checksum of the device, and then by comparing it with the returned checksum, the attestation device checks if the device is modified by attacks, and if the device is proved to be a normal device, then the attestation device approves the device.

This increases the calculating time creating addresses for approaching memory using RC4 Pseudo-random generator (PRG) by detecting approaching the modified memory when the attacker modifies the memory.

SWATT is strong for attack of presenting and pre-calculation through an arbitrary challenge that is used for the seed of Pseudo-random generator (PRG).

Although it approaches memory by randomized order, it can detect even a small change in the memory by approaching all memory at least one time through the memory of O .

The attack makes it impossible to calculate checksum within expected time period by disabling attacker to optimize the attestation function no more through device-optimized attestation function.

Using the checksum before the memory address approached for the checksum calculation is created makes the serial calculation impossible to be executed.

However, the SWATT method is not suitable for a sensor network where an approved attester by the available method doesn't exist if approved attester exists, and it is impossible for the SWATT to attest all sensor nodes 1 hop. Moreover, a sensor that attestation proves is damaged should be excluded from the network by physical removal, and a node damaged by attacks after attestation is performed is not recognizable.

III. SENSOR NODES' ATTESTATION PROTOCOL IN WIRELESS SENSOR NETWORKS

This paper suggests an inter-connective attestation protocol for sensor node suitable for wireless sensor network. This protocol is able to earlier detect a node that was damaged through neighbor node under a sensor network environment without a reliable sensor node. This protocol is for safe authentication for a sensor node. Existing research has focused on inter-connective authentication for sensor nodes and the BS instead of inter-connective authentication between sensor nodes. Therefore, when a sensor node is captured and viciously

modified, the action consequently results in problems in the network environment. The existing attestation method uses a method that proves the code of sensor node through data collective characteristics for the sensor network. In other words, the verifier regards a damaged node when there is a difference after he or she has compared the content of the memory in his or her own targeted node with those of actual memory in the current targeted node. The SWATT method carries out inter-connective attestation with the surrounding nodes assuming that there is a copy of the content for the memory in surrounding nodes, and then updates the available sensor node lists, and performs attestation for nodes that do not exist in the lists. But after inspection, a damaged node is not able to be detected with the time limit for inspecting memory. Another method is not to leave vicious program of nodes in memory space. But this method also has problems in application.

A. Assumption

This paper assumes the following sensor network environment. In other words, the sensor node has hardware limitations due to its low cost. It is difficult for a node to react to attacks coming from program modification by vicious users.

Assumption 1. There is no reliable sensor node.

Assumption 2. The sensor node has hardware limitations due to low cost.

Assumption 3. The sensor network environment is dynamically changeable (can add, remove, or modify sensor nodes).

Assumption 4. All sensor nodes include a function for attesting the memory content.

Assumption 5. An attacker is able to modify and relocate programs by accessing the captured memory area of a sensor node without limitations. But the hardware configuration is not changeable.

Assumption 6. It is impossible to attest all sensor nodes by 1 hop.

B. Proposed Sensor Nodes Attestation Method

A sensor network has a limited computing and communication resource. In order to overcome this barrier, collaboration with the surrounding nodes is required. In other words, information sharing between hierarchies is required rather than the hierarchical approach.

A sensor network generally consists of a large number of sensor nodes for exact sensing and extendibility of the sensing areas. Therefore, attackers can easily capture sensor nodes. And the attacker is able to attack the sensor node itself and sensor network through a modified attack for a sensor node. Therefore, the security of the sensor network is important.

1) Sensor Node Attestation Protocol

The 802.15.4 standards favor battery-powered devices. However, in certain applications, some of these devices could potentially be mains-powered. Battery-powered devices will require duty-cycling to reduce power consumption. These devices will spend most of their operational life in a sleep state. However, each device should periodically listen to the RF channel in order to determine whether a message is pending. This mechanism allows the application designer to decide on the balance between battery consumption and message latency. Mains-powered devices have the option of listening to the RF channel continuously [7].

The DS2401 chip used for Zigbee mote is developed by Dallas Semiconductor, and it is able to identify unique IDs in the world through the least electronic interface. The unique 64-bit registration number of this chip is recorded in its internal ROM, and this registration number consists of 8-bit product code, 48-bit serial number, and 8-bit CRC data. This can be used for identifying the PCB, network node ID, or device registration. In other words, this is a unique ID.

The attestation procedure is inter-connectively carried out between sensor nodes. The sensor node periodically sends a “hello” message to the neighbor nodes. A sending message contains a unique ID for the sensor node. If the responding node is not included in the neighbor attested node list, then attestation is carried out to recognize the node as a newly attended sensor node. The attestation procedure follows.

The channel of the sensor node is multiplexed, and randomly changed and sends a hash message.

2) Secure Authentication Protocol

Use of the MetaID as a secret key by utilizing the public key method on the hash lock is based on reverse functional calculation difficulty of one direction hash function. A hash lock can prevent other unauthorized machinery from accessing the sensor node and possibly embodied with less cost by requesting only the hash function. The sensor node verifies the sensor node with the previously registered public key (produced by using the metaID) and produces only the key (k) of each sensor node, and has a metaID = H(k) that corresponds to. At this point, H() is the function. The sensor node should obtain an authorized key by executing the transmission with the key of the corresponding sensor node to the authentication server. The executing procedure is as follows.

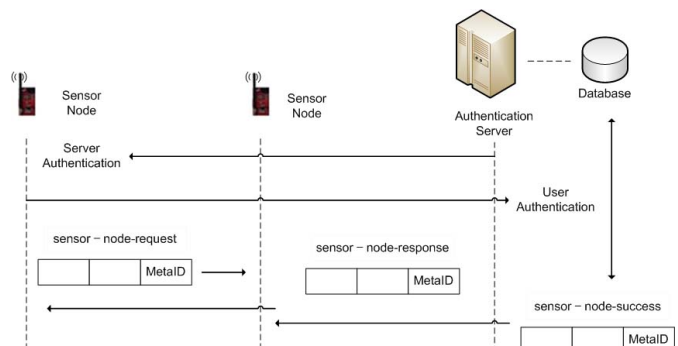


Figure 3. Secure Authentication Protocol

STEP 1. The authentication server produces the public key and secret key for the sensor node and registers it. The server requests the MetaID.

$$P(Kdb\{H(metaID)\|Kmd1\})$$

However, Kdb is the public key for the authentication server, and Kmd1 is the public key for sensor node. At this point, $P(k\{\})$ is the public key method and codes it with public key k. $H()$ is the hash function. The public key method is used to provide the code and service on the unspecific sensor node. Even though the exposed metaID of the unauthorized sensor node has been obtained, the sensor node cannot earn authentication if the corresponding value of $H(metaID)$ is not registered in the database. For this reason, the authority of $H(metaID)$ should be registered in the database and the corresponding sensor node in advance.

STEP 2. Sensor node that receipt of message is response sensor node-response message.

STEP 3. The reader or sensor node is the authentication key generated by $P(MetaID)$. $P(Kmd1\{H(DBid)\|Ksv\})$

Ksv is the server secret key, and DBid is the nonce ID of DB.

STEP 4. The sensor node executes $H(K\{\})$ by the hash function with the server key received from the database and sees the quality of the code on the value of the hash function and server with the printed ID of the database. And the sensor node sends the message 'sensor-node-response.'

$$H(Ksv\{H(DBid)\parallel query\parallel authcode\parallel Kmd2\})$$

authcode is the authentication code, and Kmd2 is the sensor node secret key.

STEP 5. The authentication server verifies the authenticcode of the sensor node. The sensor node compares the value from the authentication server's database, distinguishes if the node is valid, and sends a data message. In other words, the corresponding sensor node has access authority and indicates it made the transference legally.

$$H(Kmd2\{H(SVid)\parallel cmd1..cmd2..cmdn\})$$

SVid is the nonce ID of the server, and cmd is the command set.

A command circuit is made through a fixed server when willing to deliver any command to the corresponding sensor node in the authenticating process for the following reason. First, it can complement efficiency of the sensor node, which has limited calculation ability and is able to reject the command that has not been authorized. In other words, it can reduce equipment requisite and provide security at an adequate level for the sensor node security.

IV. SECURITY CONSIDERATION

An attacker, after capturing sensor nodes that are laid out, attempts to attack the sensor node itself or sensor network with a modified attack for the content of the sensor node memory. This enables the attacker to insert a vicious program into the ROM of the sensor node, transfer the

original code to the RAM area, execute the code, and carry out the attestation protocol through the RAM code. Therefore, the attacker can rapidly carry out attestation including an existing attestation function.

A sensor node modified by an attacker can be used for wiretapping a sending message and attack. In order to prevent this attack, the sensor node in which the vicious code is running must be identified, and those nodes excluded from the network.

Basically, physical attack against nodes is not blocked in any case. In order to prevent an attack, a hardware or software method can be used. If a hardware method is used, damage is prevented by equipping with hardware module that physically blocks node modification.

This method requires additional cost. If the software method is used, it can easily apply node modification without additional cost.

V. CONCLUSIONS

This paper suggests an inter-connective attestation protocol for a sensor node that is suitable for a wireless sensor network. This protocol is able to earlier detect a node that was damaged by a neighbor node in a sensor network environment without a reliable sensor node. This protocol is for safe authentication for the sensor node. Existing research has focused on inter-connective authentication for sensor nodes and the BS instead of inter-connective authentication between sensor nodes. Therefore, when a sensor node is captured and viciously modified, and problems result in the network environment, they can be checked. The existing attestation method uses a method that proves the code of sensor node through data collective characteristics for the sensor network. In other words, the verifier regards a damaged node when there is a difference after he or she has compared the content of memory in his or her own targeted node with those of actual memory in the current targeted node. The SWATT method carries out inter-connective attestation with surrounding nodes assuming that there is a copy of the content for the memory in the surrounding nodes, then updates the available sensor node lists, and performs attestation for the nodes that do not exist in the lists. But after inspection, a damaged node is not able to be detected within the time limit for inspecting memory. Another method is not to leave a vicious program of nodes in the memory space. But this method also has problems in application.

A sensor network has a limited computing and communication resource. In order to overcome this barrier, collaboration with surrounding nodes is required. In other words, information sharing between hierarchies is required rather than a hierarchical approach. A sensor network generally consists of a large number of sensor nodes for exact sensing and extendibility of sensing areas. Therefore, attackers can easily capture sensor nodes. And an attacker is able to attack the sensor node itself and the sensor network through a modified attack on the sensor node. Therefore, the security of the sensor network is important.

As mentioned above, because there is a periodic simple attestation procedure between sensor nodes and sensor node

attestation. The proposed method is easy and rapid to identify which is captured by attacker, thus security of sensor network is attainable.

ACKNOWLEDGMENT

This work was supported by Brain Korea 21 project in 2009.

REFERENCES

- [1] G.M. Ben Ezovski, S.E. Watkins, "The Electronic Sensor Node and the Future of Government-Issued RFID-Based Identification", RFID, 2007. IEEE International Conference, pp 15-22, 2007.
- [2] I.F. Akyiliz, W. Su, Y.Sankarasubramaniam and E. Cayirci, "A Survey on Sensor Network", IEEE Communication Magazine, pp 102-114, 2002.
- [3] E. Shi, and A. Perrig, "Designing Secure Sensor Networks", IEEE Wireless Communication, pp 8-43, 2004.
- [4] T.C. Group, "Trusted Platform Module (TPM) Specifications, Techniques", ESAS 2007, LNCS 4572, pp 203-217, 2007.
- [5] A. Seshadri, A. Perrig, L. V. Doorn, and P. K. Khosla, "SWATT: SoftWare-based ATTestation for Embedded Devices", IEEE Symposium on Security and Privacy, pp 272-282, 2004.
- [6] Y. Yang, X. Wang, S. Zhu, and G. Cao, "Distributed Software-based Attestation for Node Compromise Detection in Sensor Networks", SRDS 2007, pp 219-230, 2007.
- [7] A. Perrig, R. Szewczyk, V. Wen, D. Culler and J. D. Tygar, "SPINS: Security Protocols for Sensor Network", Wireless Network Journal (WINE), pp xxx-xxx, 2002.