Security for IEEE P1451.0-Based IoT Sensor Networks

Ke Zhou
School of Electronic Information and Electrical Engineering
Shanghai Jiao Tong University
Shanghai, China
zhouke1998301@sjtu.edu.cn

Jun Wu
School of Electronic Information and Electrical Engineering
Shanghai Jiao Tong University
Shanghai, China
junwuhn@sjtu.edu.cn

Kang B. Lee
IEEE Life Fellow
Gaithersburg, Maryland USA
kang.lee@ieee.org

Eugene Y. Song
Engineering Laboratory
National Institute of Standards and Technology (NIST)
Gaithersburg, MD, USA
eugene.song@nist.gov

IECON 2021 - 47th Annual Conference of the IEEE Industrial Electronics Society | 978-1-6654-3554-3/21/$31.00 ©2021 IEEE | DOI: 10.1109/IECON48115.2021.9589277

***Abstract*—The challenges of the Internet of Things (IoT) sensor networks include connectivity, interoperability, security, and privacy. The Institute of Electrical and Electronics Engineers (IEEE) P1451.0 standard is being revised based on these challenges and requirements to achieve sensor data interoperability and security for IoT applications. This paper analyzes the security requirements of sensor networks for IoT applications and proposed security solutions for IEEE P1451.0-based IoT sensor networks. It specifies security policies and levels of IEEE P1451.0-based sensor networks to meet the security requirements and defines security transducer electronic data sheets (TEDS) to describe security protocol information for IEEE P1451.0-based sensor networks. An implementation of the security TEDS for IEEE P1451.0 and P1451.5-802.11 wireless sensor networks is provided to illustrate how to access security TEDS that contain detailed security parameters and information to achieve sensor data security and interoperability.**

Keywords—IEEE P1451.0, security, sensor network, Internet of Things, TEDS.

I. INTRODUCTION

The Internet of Things (IoT) is a system of uniquely identifiable "Things" or devices that are interconnected to the Internet and can share sensing and actuation data and information. The challenges of IoT sensor networks include connectivity, interoperability, security, and privacy. IoT cybersecurity is the act of securing IoT devices and the sensor networks they are connected to. Along with the growth of IoT, new security issues arise while traditional security issues become more severe. The main reasons are the heterogeneity and the large scale of connected objects [1]. As a fusion of heterogeneous networks, IoT not only encounters the same security problems with sensor networks, mobile communication networks, and the Internet but also more particular ones, such as privacy protection problems, heterogeneous network authentication, access control problems, as well as information storage and management [2].

Networked sensors connected using wired or wireless means can be used in many applications in IoT, such as aerospace, smart homes, and industrial automation [3]. To address the requirements of IoT, Industrial Internet of Things (IIoT), smart grid, and cyber-physical systems (CPS) applications via different types of network interfaces, the Institute of Electrical and Electronics Engineers (IEEE) P1451 family of standards on smart transducer interfaces for sensors and actuators have defined standards specifications for device-level and network-level interfaces to fulfill these needs.

The IEEE P1451 family of standards architecture is shown in Fig.1. The family of standards is uniquely defined with device-level interfaces, such as the mixed-mode transducers interface (P1451.4), wired (P1451.2) and wireless interfaces (P1451.5), and Radio-frequency identification (RFID)-to-sensor interface (P1451.7). And it is also defined with network-level interfaces such as P1451.1.4 extensible messaging and presence protocol (XMPP), P1451.1.5 simple network management protocol (SNMP), and P1451.1.6 message queue telemetry transport (MQTT) for IoT applications (1451 clients) to access sensor data and metadata information to and from the devices as well as P1451.99 (network harmonization interface) to exchange these P1451 data and information with other non-1451 IoT networks. All these interfaces shown in Fig. 1 are based on the core of the family of standards, IEEE P1451.0, which provides common functions, network services, transducer services, and transducer electronic data sheets (TEDS) formats for members of the IEEE P1451 family of standards to be interoperable in both network interfaces and transducer interface [4]. It defines the common functions and characteristics that are to be performed by a network-capable application processor (NCAP) that is a 1451 server or a gateway of IEEE P1451.0 standard-based sensor networks. It defines a set of network services application programming interface (API) that includes a set of requests and responses to access sensor data and TEDS data from the NCAP (1451 server) for IoT applications (1451 clients). It also defines the common functions and characteristics that are to be performed by a transducer interface module (TIM). It defines a set of transducer services that include a set of commands and replies to facilitate the setup and control of the TIM as well as reading and writing the data used by the system. APIs are defined to facilitate communications with the TIM and with applications. It also specifies the TEDS formats. These standards also define global identity, security, and time

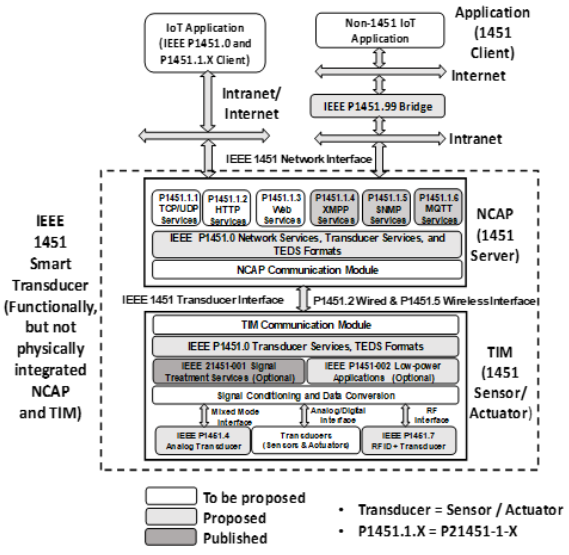

Fig. 1. Architecture of suite of IEEE P1451 standards.

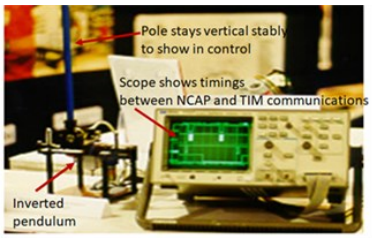

Fig. 2. IEEE 1451 NCAP and TIM combination showing real-time control of an inverted pendulum.

synchronization for IEEE P1451.0-based local-area network (LAN) and wide-area network (WAN) sensor networks. The objective of IEEE P1451.0 is to achieve sensor data interoperability in the network interface and transducer interface. IEEE P1451.0 enables the access of sensors and actuators data and information and passes them to IoT, IIoT, and CPS clients and applications via all these network interfaces mentioned above. An IEEE 1451 NCAP and TIM combination has demonstrated a real-time control of an inverted pendulum, which is a pendulum with its center of mass above its pivot point. The inverted pendulum is unstable and it needs to be controlled to stay up vertically and stably by a motor control system. This IEEE 1451-based motor-controlled, inverted pendulum system shown in Fig. 2 [5] has illustrated a typical high-speed control application in IoT with sensors and actuators. Thus IEEE P1451 standards work well to support sensing and actuation functions for IoT and its control bandwith is mainly based on the capability of controller hardware selected. The IoT applications of IEEE P1451.0-based sensor networks can reduce human errors by using TEDS to perform self-configuration, improve and maintain sensor measurement accuracy by using calibration TEDS data, ease field installation, upgrade, and maintenance by the plug and play of replacement devices, and thus reducing the total life-cycle costs of IoT sensor systems.

The deployment of IEEE 1451 smart transducers and sensor networks for IoT can help achieve sensor data interoperability and plug-and-play capability. Standardized messaging can be used to access sensor data in a standardized format and to command actuation in IoT systems. IoT applications can access sensors and actuators connected to the TIM (or simply referred to as 1451 sensor/actuator node) via the NCAP (referred to as 1451 server or network node). Like other IoT systems, IEEE P1451.0-based sensor networks could be exposed to increased security threats that have potential impacts in the areas of confidentiality, integrity, and availability of the networks. Therefore, there is a need to develop security requirements and specifications for the secure operation of IEEE P1451.0-based sensor networks.

This paper focuses on the security of IEEE P1451.0-based sensor networks, including security requirements of IEEE P1451.0-based WAN interfaces and LAN interfaces, the proposed security solutions for IEEE P1451.0-based sensor networks, and the implementation of IEEE P1451 security levels. This paper is organized as follows. Security requirements of IEEE P1451.0-based sensor networks are analyzed in Section II. Section III describes proposed security solutions for IEEE P1451.0 sensor networks. The security TEDS implementation of IEEE P1451.0 and P1451.5 - 802.11 wireless sensor networks is provided in Section IV. Section V provides the conclusion.

II. Security Requirements of IEEE P1451.0-Based Sensor Networks

A. *Architecture of Security for IEEE P1451.0-Based Sensor Networks*

Fig. 3 shows an architecture of security of IEEE P1451.0 standard-based sensor networks for IoT applications [5]. As shown in Fig. 3, an IEEE P1451.0 and P1451.1.X standards-based WAN consists of a few of IoT applications (1451 clients), and a set of NCAPs (1451 server, or network gateway node). These NCAPs are connected with the IoT applications via Internet/Intranet (e.g., Ethernet or cellular). The communications between IoT applications and NCAPs are based on IEEE P1451.0 network services and IEEE P1451.1.X interfaces. Also, an IEEE P1451.0 and P1451.5.X standards-based wireless LAN (WLAN) consists of an NCAP (1451 server) and a set of wireless TIM (WTIM). These WTIMs are connected with the NCAP via wireless mediums defined in IEEE P1451.5.X interfaces (e.g., 802.11, Bluetooth, ZigBee, 6LowPAN, NB-IoT, SigFox, and LoRa WAN). The communications between the NCAP and WTIMs are based on IEEE P1451.0 transducer services and IEEE P1451.5.X interfaces.

B. *Security Requirements of IEEE P1451.0-Based Sensor Networks*

IEEE P1451.0-based sensor network security is the act of securing IoT devices and the networks they are connected to. The key requirements for any IoT security solution are device and data security, including the authentication of devices and confidentiality and integrity of data [6].

1) Security Requirements of IEEE 1451 WAN Interfaces

The WAN interfaces have a large number of devices, and each has to be authenticated to ensure the right devices are using the network.

a) Application: The application will be software installed on a computer to provide command and control information to the sensors via the NCAP (gateway) and to receive and process sensor data for monitoring and control applications and display results. The security requirements of the applications are:

- The integrity of application software can be verified.
- The identity of applications connected to the NCAPs can be authenticated.
- The integrity of the received data can be verified [7].
- The source of the received data can be authenticated as a legitimate NCAP.

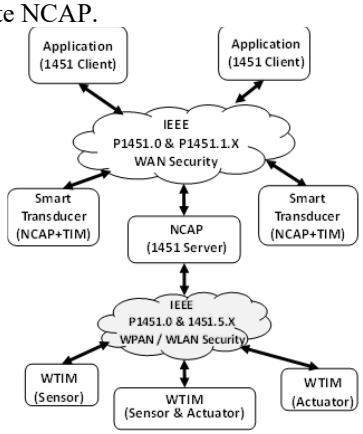

Fig. 3. Architecture of security for IEEE P1451.0-based sensor networks.

- Applications need to make sure the traffic is not overloaded.
- Data stored in application need to be protected.
- Data transferred in application need to be encrypted.

b) NCAP in WAN: The NCAP will forward sensor data to the application (1451 client) for processing. Similarly, the NCAP may receive command and control information from the application (1451 Client) to send to the appropriate TIM. The security requirements of NCAPs are:

- The identity of NCAPs connected to the IoT applications should be authenticated by applications.
- NCAPs should make sure the network traffic is not overloaded. Data transferred in NCAPs need to be encrypted.
- The source of the received data can be authenticated as a legitimate application or NCAP [8].
- NCAPs authorize IoT applications and ensure applications only get the data they are authorized to access [9].

2) Security Requirements of IEEE 1451 LAN Interfaces

a) TIMs: The TIMs mainly refer to 1451 wireless sensors and actuators with resource-limited. The security requirements of TIMs are:

- The integrity of the LAN firmware, configuration, software, and hardware circuits can be verified [10].
- The identity of TIMs connected to the NCAPs can be verified by NCAPs.
- TIMs only respond to messages from authenticated and authorized devices.
- TIMs only transmit data to the desired and authorized devices. The data is secure and accessible only to authorized users [11].
- TIMs do not allow the collected data to be accessed by neighboring nodes [11].

b) NCAP in LAN: The NCAP will be a wireless radio configured to receive and aggregate signals from the WTIMs. The NCAP will forward sensor data to the application (1451 client) for processing and data fusion. Similarly, the NCAP may receive command and control information from the application (1451 Client) to send to the appropriate TIM. The security requirements of NCAP in LAN are as follows:

- The payloads of the packets in the LAN interface should be encrypted [12].
- The identity of NCAPs connected to TIMs should be authenticated by TIMs.
- The source of the received data can be authenticated as a legitimate TIM or NCAP [8].
- Ensure the data transmitted to TIMs or the other NCAPs is within the scope that they are authorized to access [13].
- The LAN interface resiliency maintains a given security level over the network even when a TIM is compromised [14].

III. Proposed Security Solutions for IEEE 1451.0 Sensor Networks

A. Security Policies of IEEE 1451.0-based Sensor Networks

IEEE 1451 sensor networks' security policies are divided into three main categories: encryption, authentication, and authorization.

1) Encryption: Encryption is the process of encoding information. Since data may be visible on the IoT, sensitive information such as passwords and personal communication may be exposed to potential interceptors. On the IEEE 1451 sensor networks, the application of encryption is to ensure the data security of the communication channel. In addition to encrypting the primary data, it is also important to encrypt data of any available secondary communication channels.

2) Authentication: Authentication mechanisms in IEEE P1451.0-based sensor networks include identity verification and integrity checking mechanisms. Identity verification mechanisms are to verify the identity of sensor network components, i.e. TIMs, NCAPs, and applications (1451 clients) that can be authenticated with each other. Integrity checking mechanisms are used to verify software, firmware, and information integrity [6].

3) Authorization: Authorization determines and enforces the access rights of an IoT entity, allowing the entity to use specific resources. Authorization provides a mechanism to bind a specific device to certain permissions. IoT devices use the authorization process to do role-based access control and ensure that devices only have access and permission to do exactly what they need. Only authorized devices can interact with other devices, applications, and cloud accounts.

B. Security Levels of IEEE P1451.0-based Sensor Networks

Based on the security policies, six security levels of IEEE 1451 sensor networks are shown in Table I. Except level 0, which means no security, each security level is a combination of the three security policies. Generally speaking, higher security levels including more criteria are considered more secure than low security levels.

1) Level 0: Sometimes embedding security standards can bring a serious load that could affect the performance of low-capability sensor networks. Meanwhile, security problems are not necessarily needed in some sensor network applications. That means some sensor networks do not require any security policies. Thus security level 0 represents no security policies that need to be deployed in the specific IEEE 1451 sensor network.

2) Level 1: Security level 1 supports only encryption, which is used to keep IEEE 1451 sensor network data encrypted. For example, security level 1 can ensure the collected data in the NCAP is protected at rest or in transit. Especially, devices' sensitive information should be protected from being leaked by encryption in the progress of storage, transmission, and access. Security level 1 is suitable for sensor networks whose security requirements contain only confidentiality.

TABLE I. Security Level for IEEE P1451.0-based Sensor Networks

Security Level	Encryption	Authentication	Authorization
0			
1	x		
2		x	
3	x	x	
4		x	x
5	x	x	x

TABLE II. SECURITY TEDS.

Field type	Field name	Description	Data type	# octet	M/O	Range
—		Length	UInt32	4		
0-2	—	Reserved	—	—		
3	TEDSID	TEDS Identification Header	UInt32	4	M	
4-9	—	Reserved	—	—		
Security related information						
10	Level	Security level	UInt8		M	0-5
11	NumOf Protocols	Number of Security Protocols	Uint8		M/O	0-10
12	SecurityStd Name1	Security standard Name 1	UInt8	1	M/O	0-100
13	SecurityStd Version1	Security Standard Version 1	UInt8	1	M/O	0-10
14	SecurityStd Name2	Security Standard Name 2	UInt8	1	M/O	0-20
15	SecurityStd Version2	Security Standard Version 2	UInt8	1	M/O	0-10
…	…					
2*N+10	SecurityStd NameN	Security Standard Name N	UInt8	1	M/O	0-20
2*N+11	SecurityStd VersionN	Security Standard Version N	UInt8	1	M/O	0-10
2*N+12-127	—	Reserved	—	—		
128-255	—	Open to manufacturers	—	—		
—		Checksum	UInt16	2		

3) Level 2: In some sensor network scenarios, data integrity and availability instead of confidentiality are considered. Only authentication is provided in security level 2. Users can choose this security level when access control or integrity of data has to be ensured. For instance, when the identity of NCAPs connected to the IoT and the applications connected to the NCAPs must be authenticated, this security level can be very helpful.

4) Level 3: In most cases, sensor networks require both encryption and authentication to ensure security. Security level 3 is a combination of these two policies i.e., encryption and authentication. By adopting security level 3, the network traffic can be encrypted and the access authentication can be conducted by NCAPs to certain TIMs or applications.

5) Level 4: Authentication and authorization are often used together. Thus security level 4 combines authentication and authorization to provide a higher security level for the operation of sensor networks. Authentication realizes access control by a certificate or a key, while authorization controls the resources' access rights in the form of permissions. Security level 4 requires NCAPs to provide an authorization identity to other authenticated devices, therefore allowing them to get access to data in a broader network.

6) Level 5: When IEEE 1451 sensor networks are deployed in some important scenarios such as health condition monitoring, smart grid, and aerospace, security level 5 needs to be applied to satisfy the highest security demands. This security level is made up of encryption, authentication, and authorization in order to protect sensor networks from malicious attacks.

C. Security TEDS

TEDS is used to describe the characteristics of the transducers in IEEE 1451 sensor networks. The amount of detail held within the TEDS varies with each application, but critical information is always present. The content and structure of this TEDS are defined in the IEEE P1451.0 standards, including standard protocol name, version, profile name, and main characteristics of the protocol. The security TEDS is accessed using a Query TEDS command, a Read TEDS segment command, a Write TEDS segment command, or an Update TEDS command. The content and structure of security TEDS are shown in Table II. Security TEDS first indicates how many security protocols are employed through the entry NumOfProtocols, and then provides detailed information of each protocol, respectively, by SecurityStdName entry and SecurityStdVersion entry.

IV. SECURITY TEDS IMPLEMENTATION OF IEEE P1451.0 AND P1451.5 - 802.11 WIRELESS SENSOR NETWORKS

A. Architecture of IEEE P1451.0 and P1451.5 - 802.11 Wireless Sensor Network

An experimental system shown in Fig. 4 was put together to demonstrate the proper access of a security TEDS in an IEEE P1451.0 and P1451.5-802.11 based wireless sensor network. Table III shows a number of security protocols for IEEE P1451.5 - 802.11, which will help to set up security level for IEEE P1451.5-802.11 based on different security policy criteria listed in Table III. It showed that an NCAP can get the information of the security protocol deployed in the IEEE 1451 sensor networks. This security information can be obtained by sending a request for a security TEDS to the TIM where the TEDS is stored. The architecture for this system is shown in Fig. 4, and the implementation is made up of the following steps.

- The NCAP obtains the security TEDS used in this sensor network by sending a Read TEDS request command to the TIM. The command argument values are stored in the command header.
- According to the command arguments, the NCAP can choose which TIM, if more TIMs are used in the system, to send the command to. Then the NCAP encodes both the command header and command body into a binary code and then sends the message to the selected TIM.
- Once the TIM receives the call function message, it decodes the message and starts to prepare a reply message. After verifying the TEDSAccessCode, the TIM encodes the stored security TEDS and reply message header, and finally sends the entire packet to the NCAP, by which the security TEDS is forwarded.

B. Security TEDS Implementation

In the implementation system, we use two connected Ubuntu** hosts to simulate an IEEE P1451.0-based sensor network, one as a TIM (server) and the other as an NCAP (client). Since the communication protocol used between the NCAP and TIM is Wi-Fi, the security TEDS stored in TIM is the Wi-Fi Protected Access (WPA) TEDS. In this WPA TEDS, the security standard is WPA3-Enterprise 192-bit mode. This protocol can realize encryption by advanced encryption standard (AES)-256- galois/counter mode protocol (GCMP)

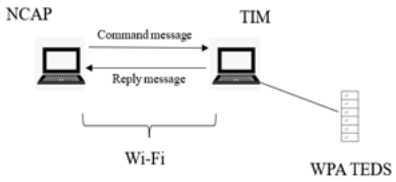

Fig. 4. Architecture of IEEE P1451.0 and P1451.5 - 802.11 wireless sensor network.

TABLE III. SECURITY PROTOCOLS FOR IEEE P1451.5 - 802.11

Security Policy	No	Security scheme	Encryption	Authentication	Authorization
Encryption	0				
	1	AES	x		
	2	AES-CCMP	x		
Authentication	0				
	1	extensible authentication protocol (EAP)		x	
	2	light EAP (LEAP)		x	
	3	EAP- transport layer security (TLS)		x	
	4	protected EAP (PEAP)			
	5	WPA	x	x	
	6	temporal key integrity protocol (TKIP)	x	x	
	7	wired equivalent privacy (WEP)	x	x	
Authorization	0				
	1	WLAN authentication and privacy infrastructure (WAPI)	x	x	x

TABLE IV. READ TEDS COMMAND MESSAGE STRUCTURE

Command class (1)
Command function (2)
Xdcr service message type (1) (command)
Length
TIM ID Destination TransducerChannel Number (0) UInt8 TEDSAccessCode : TEDS access code (16) UInt32 TEDSOffset: TEDS Segment offset.

TABLE V. REPLY MESSAGE STRUCTURE

Command class (1)
Command function (2)
Message type (2)
Length
Error code (Success/Fail Flag) Source TransducerChannel Number (0) UInt32 TEDSOffset : TEDS Segment offset (0 to [current size – 1]) OctetArray RawTEDSBlock:TEDS data octets.

and authentication by secure hash algorithms (SHA)-384, thus the TEDS security level is set at level 3.

C. Security TEDS Access based on IEEE P1451.0 Transducer Services

In the implementation system, the NCAP can get the security TEDS by sending the Read TEDS command to the TIM. As shown in Table IV and Table V, both command message and reply message consist of a message header and a message body. For a Read TEDS command, The value of each argument is specified in Table IV, and the TEDS access code for security TEDS is 16. The content of WPA TEDS is contained in the reply message body and the message header is specified in Table V.

For message transmission, a client-server TCP connection is established between the NCAP and TIM. In this case, the NCAP is a client that sends a command message to the TIM, the server. Respectively, the TIM sends a reply message back to the NCAP via the Wi-Fi connection.

According to the argument TIM ID, NCAP decides which TIM to send the command message to, then the command message is encoded by the NCAP, and transmitted to the TIM through a TCP packet. After the TIM receives the command message, it decodes and verifies the command parameter value and TEDS access code. If the verification is correct, the TIM encodes the reply message and sends it back to the NCAP by a TCP packet. At the end of this communication exchange, the NCAP receives the reply message and decodes it to obtain the security TEDS information.

D. Testing Results of Security TEDS Implementation

The message transmission process between the NCAP and TIM is presented in Fig. 5 and Fig. 6. The NCAP sends an encoded command message to the TIM for the security TEDS. Then, TIM decodes the command message and verifies the parameters. After the verification is confirmed, the TIM sends an encoded reply message which contains the WPA TEDS to NCAP. Finally, the NCAP decodes the reply to the message and gets the WPA TEDS.

The specific information of the Wi-Fi security protocol used in the sensor network can be obtained from the WPA TEDS, which can enable secure plug-and-play. For example, the client can check its security requirements to ensure that the security standard version used in the network can fulfill the requirements, then decides whether to connect to the sensor network or not. Besides, the client can install a SHA-384 suite to match the security standard known from the TEDS. Otherwise, it can't be authenticated successfully in the Wi-Fi network.

In Fig. 5, the TIM is the server in the TCP connection. It receives a Read TEDS command message from the NCAP. After verifying command parameters, the TIM sends an encoded reply message containing the WPA TEDS back to NCAP. In Fig. 6, the NCAP is the client in the TCP connection. It sends an encoded Read TEDS command to the TIM and receives the reply message. The NCAP gets the WPA TEDS from the TIM and then decodes the reply message.

```
tim1@ubuntu:~/Downloads$ python3 server.py
Server is running...
Accept new connection from 192.168.70.138:38594.
Command message reveived.
TIMID  01
Destination TransducerChannel Number  0
TEDSAccessCode  16
Sending reply message...
length of reply message  1131
Sent successfully.
Connection from 192.168.70.138:38594 closed.
```

Fig. 5. Screenshot of TIM communication with NCAP.

```
(base) keyi@ubuntu:~/Downloads$ python3 client.py
Command class: 1
Command function: 2
Xdcr service message type: 1
TIM ID: 01
Destination TransducerChannnel Number: 0
TEDSAccessCode: 16
Length =  14
The following command message will be encoded:
12114010160000
Sending command message...
Sent successfully
```

Fig. 6. Screenshot of NCAP communication with TIM (server).

```
Receiving reply message...
Received successfully.
```

WPA TEDS

FIELD TYPE	FIELD NAME	DESCRIPTION	DATA TYPE	# OCTET	M/O	RANGE	VALUE	DESCRIPTION
–		Length	UInt32	4				
0-2	–	Reserved	–	–				
3	TEDSID	TEDS Identification Header	UInt8	4			5 16 1 1	
4-9	–	Reserved	–	–				
Security related information								
10	Level	Security level	UInt8		M	0-5	3	Level 3
11	NumOfProtocols	Number of Security Protocols	UInt8		M/O	0-10	1	1 protocol
12	SecurityStd Name1	Security standard Name 1	UInt8	1	M/O	0-100	5	WPA
13	SecurityStd Version1	Security standard version 1	UInt8	1	M/O	0-10	3	WPA3-Enterprise 192-bit mode
21-127	–	Reserved	–	–				
128-255	–	Open to manufacturers	–	–				
–		Checksum	UInt16	2				

Fig. 7. WPA TEDS content.

Fig. 7 shows the security TEDS contents that include security level: 3, security protocol name: WPA (5), and security protocol version: 3. Security level 3 includes encryption and authentication as shown in Table I, which are provided by the WPA 3 security protocol. The TEDS ID consists of four fields: 1451 family (5), security TEDS access code (16), Version of IEEE 1451.5 (1), and tuple length (1).

V. CONCLUSION

This paper describes the security requirements for the IEEE P1451.0-based IoT sensor networks. Security requirements of the IEEE P1451.0 WAN and LAN interfaces are analyzed. Then security solutions of IEEE P1451.0-based IoT sensor networks are proposed according to these security requirements, which include security policies (i.e., encryption, authentication, and authorization) and six security levels based on different criteria and their combinations of these security policies. The various security policies and levels provide users a wide range of options for their desired security solutions based on their application specific security needs. The implementation of the security TEDS of IEEE P1451.0 and P1451.5-802.11 wireless sensor network was described in the paper. The operation of the NCAP obtaining the security TEDS information from the TIM by sending a command request for the security TEDS to the TIM via the IEEE P1451.5-802.11 wireless interface was explained and shown to be functioning properly. As an example, the security TEDS information of the IEEE P1451.5-802.11 security protocol between the NCAP and TIM is also described in the paper.

** Certain commercial products or company names are identified here to describe our study adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the products or names identified are necessarily the best available for the purpose.

REFERENCES

[1] Z. Zhang, M. C. Y. Cho, C. Wang, C. Hsu, C. Chen and S. Shieh, "IoT Security: Ongoing Challenges and Research Opportunities," 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, 2014, pp. 230-234.

[2] K. Zhao and L. Ge, "A Survey on the Internet of Things Security," 2013 Ninth International Conference on Computational Intelligence and Security, 2013, pp. 663-667.

[3] J. Wu, M. Dong, K. Ota, J. Li, W. Yang, "Application-Aware Consensus Management for Software-defined Intelligent Blockchain in IoT," IEEE Network, vol. 34, no. 1, pp. 69-75, 2020.

[4] IEEE P1451.0 [Online]. Available: https://standards.ieee.org/project/1451_0.html.

[5] Kang B. Lee, IEEE 1451 Smart Transducer Interface Standards for IoT, IIoT, and CPS, [Online]. Available: http://sagroups.ieee.org/1451-9/wp-content/uploads/sites/132/2020/09/IEEE-P1451-Smart-Transducer-Standard-for-IoT-2020-1-10.pdf.

[6] Jeffrey Cichonski, Jeffrey Marron, and Nelson Hastings, Security for IoT Sensor Networks, National Institute of Standards and Technology, February 2019. [Online]. Available: https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/iot-sniot-sensor-network-project-description-draft.pdf.

[7] S. N. Swamy, D. Jadhav and N. Kulkarni, "Security threats in the application layer in IOT applications," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2017, pp. 477-480.

[8] John Moo, Establishing principles for Internet Of Things security, IoT Security Foundation [IoTSecFoundation]. [Online]. Available: https://www.iotsecurityfoundation.org/wp-content/uploads/2015/09/IoTSF-Establishing-Principles-for-IoT-Security-Download.pdf.

[9] P. Saint-Andre, Extensible Messaging and Presence Protocol (XMPP): Core, Internet Engineering Task Force (IETF), Cisco, March 2011. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc6120.

[10] Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou, Sensor Network Security: A Survey, IEEE communications surveys & tutorials, vol. 11, no. 2, second quarter 2009.

[11] S. Vashi, J. Ram, J. Modi, S. Verma and C. Prakash, "Internet of Things (IoT): A vision, architectural elements, and security issues," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2017, pp. 492-496.

[12] Juha T. Vainio, Bluetooth Security, [Online]. Available: http://www.yuuhaw.com/bluesec.pdf.

[13] L. Guo, J. Wu, Z. Xia, J. Li, "Proposed Security Mechanism for XMPP-Based Communications of ISO/IEC/IEEE 21451 Sensor Networks," IEEE Sensors Journal, vol. 15, no. 5, pp. 2577-2586, 2015.

[14] C. Hennebert and J. D. Santos, "Security Protocols and Privacy Issues into 6LoWPAN Stack: A Synthesis," in IEEE Internet of Things Journal, vol. 1, no. 5, pp. 384-398.