PT. 4. WIRELESS VIDEO SENSOR NETWORKS, COMMUNICATIONS AND CONTROL pdf

1: Home Page International Journal of Sensors, Wireless Communications and Control

The Wireless Control Network: A New Approach for Control over Networks Abstract We present a method to stabilize a plant with a network of resource constrained wireless nodes.

Correspondence should be addressed to Ming Luo ; moc. This is an open access article distributed under the Creative Commons Attribution License , which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. Nevertheless, almost all of these schemes assume that communication nodes in different network domains share common system parameters, which is not suitable for cross-domain IoT environment in practical situations. To solve this shortcoming, we propose a more secure and efficient access control scheme for wireless sensor networks in the cross-domain context of the Internet of Things, which allows an Internet user in a certificateless cryptography CLC environment to communicate with a sensor node in an identity-based cryptography IBC environment with different system parameters. Moreover, our proposed scheme achieves known session-specific temporary information security KSSTIS that most of access control schemes cannot satisfy. Performance analysis is given to show that our scheme is well suited for wireless sensor networks in the cross-domain context of the IoT. Introduction Wireless sensor network WSN is a distributed network which contains a large number of sensor nodes. We can collect the target data through the sensor nodes to obtain valuable information. The integration of WSN applications and low-power sensing nodes with the Internet may be accomplished with various approaches and strategies [1], and the popular integration solutions include cloud-based integration approaches [2 , 3], front-end proxy integration approaches [4], architecture frameworks [5], and the integration via standard Internet communication protocols [6 , 7]. In the cloud-based integration solution, some important security requirements including privacy, trust, and anonymity cannot be addressed. This approach also does not support the secure integration with data sources from other sensing devices or heterogeneous WSN domains. For the front-end proxy integration solution, the wireless sensor nodes communicate with the Internet hosts through a proxy server; thus this integration approach does not support direct communications between WSN nodes and Internet hosts, and the shortcoming of this approach is that the proxy server is vulnerable to cyberattacks and may become the bottleneck. In the integration solution via standard Internet communication protocols, most of approaches employ specialized middleware layers instead of supporting generic Internet communication mechanisms that can implement heterogeneous applications. However, these proposed solutions developed in the context of the architecture frameworks currently do not support Internet communications in WSN environments. For the integration via standard Internet communication protocols, a large number of access control schemes using public key infrastructure PKI are proposed. PKI, however, has a serious problem of certificate management. Subsequently, a series of access control schemes using identity-based cryptography IBC or certificateless cryptography CLC are designed, and even a new idea of integrating IBC with CLC into an access control scheme is introduced. In particular some access control schemes using heterogeneous signcryption schemes are generated, in which an Internet sender as part of IoT belongs to the CLC environment and a wireless sensor receiver is in the IBC environment. However, almost all of these access control schemes assume that communication nodes share common system parameters in different network domains, which are not suitable for cross-domain IoT environment in practical situations. Moreover, we find that most of these schemes cannot satisfy known session-specific temporary information security KSSTIS, which means that the attacker cannot obtain the plaintext message when the ephemeral key and the access request message are leaked. Thus, it is necessary to design a more secure and efficient access control scheme and make it more suitable for wireless sensor networks in the cross-domain context of the IoT. Related Work Zhou et al. However, to authenticate a sensor node, the scheme of Zhou et al. Next, Huang [9] proposed an efficient access control protocol EACP based on the EC, which is quite adequate for low-powered sensor nodes. However, Lee et al. In , Chen et al. Recently, Kumar et al. However, these schemes above

cannot provide message confidentiality and unforgeability at the same time. In order to simultaneously authenticate the sensor node and protect the confidentiality of messages with a low cost, Yu et al. Signcryption performs the signature and the encryption in one logical step. Compared with the signature-then-encryption method, signcryption has less cost. In order to avoid this problem and reduce the burden on traditional PKI, identity-based public key cryptography IBC and certificateless public key cryptography CLC were proposed, where certificate used in PKI is not needed. Heterogeneous signcryption allows the sender to send a message to the receiver in different security domain. In , Li et al. Our Contribution In this paper, we propose an access control scheme for WSNs in the cross-domain context of the IoT using heterogeneous signcryption. Compared with NACS scheme [21] through performance analysis, our scheme has the following merits: But for the Unsigncryption algorithm, our scheme only needs three bilinear pairings computations, while the NACS scheme requires four. As we all know, bilinear pairing computation is the most expensive operation in a signcryption scheme from bilinear pairing; our scheme satisfies the known session-specific temporary information security attribute. Organization The remainder of our paper is organized as follows. The preliminaries for network model, bilinear pairings, and difficult mathematical problems are given in the next section. The third section elaborates on the definition of the cross-domain heterogeneous signcryption CDHSC , proposes a specific CDHSC scheme, and gives the security analysis of the proposed scheme. In the fourth section we propose a secure and efficient access control scheme for wireless sensor networks in the cross-domain context of the IoT and perform an efficiency analysis on it. In the last section, we make a summary. Preliminaries In this part, we give the basic network model of access control scheme, some prior knowledge of bilinear pairings, and difficult mathematical problems. The KGC is responsible for producing a part of the private key of Internet users, and the other part of the private key is generated by the users themselves. In the KGC environment, when an Internet user wants to access the information collected by the sensor nodes from WSN, he needs to signcrypt and submit the query message to the gateway. The gateway belonging to this WSN will first authenticate the access request message from the Internet user. If the verification is passed, the gateway will forward the query message to the WSN. Then the WSN transmits the collected data to the Internet user with unsigncryption key. Otherwise, gateway refuses to provide the service. In the network model of access control, the access request message generated by the Internet user should satisfy confidentiality, integrity, authentication, nonrepudiation, and known session-specific temporary information security KSSTIS simultaneously when it is transmitted to the gateway. Figure 1 shows the overview of the network model.

PT. 4. WIRELESS VIDEO SENSOR NETWORKS, COMMUNICATIONS AND CONTROL pdf

2: Wireless Mesh Networks | Sensors Magazine

Autoplay When autoplay is enabled, a suggested video will automatically play next. Up next S-MAC (Sensor- Medium Access Control) Protocol for Wireless Sensor Network - Duration:

There are an increasing number of small companies producing WSN hardware and the commercial situation can be compared to home computing in the s. Many of the nodes are still in the research and development stage, particularly their software. Also inherent to sensor network adoption is the use of very low power methods for radio communication and data acquisition. The Gateway acts as a bridge between the WSN and the other network. This enables data to be stored and processed by devices with more resources, for example, in a remotely located server. Wireless[edit] There are several wireless standards and solutions for sensor node connectivity. Thread and ZigBee can connect sensors operating at 2. With the emergence of Internet of Things , many other proposals have been made to provide sensor connectivity. Wi-SUN [19] connects devices at home. WSNs may be deployed in large numbers in various environments, including remote and hostile regions, where ad hoc communications are a key component. For this reason, algorithms and protocols need to address the following issues: Increased lifespan Robustness and fault tolerance Self-configuration Lifetime maximization: To conserve power, wireless sensor nodes normally power off both the radio transmitter and the radio receiver when not in use. Recently, it has been observed that by periodically turning on and off the sensing and communication capabilities of sensor nodes, we can significantly reduce the active time and thus prolong network lifetime. However, this duty cycling may result in high network latency, routing overhead, and neighbor discovery delays due to asynchronous sleep and wake-up scheduling. These limitations call for a countermeasure for duty-cycled wireless sensor networks which should minimize routing information, routing traffic load, and energy consumption. Researchers from Sungkyunkwan University have proposed a lightweight non-increasing delivery-latency interval routing referred as LNDIR. This scheme can discover minimum latency routes at each non-increasing delivery-latency interval instead of each time slot. Simulation experiments demonstrated the validity of this novel approach in minimizing routing information stored at each sensor. Furthermore, this novel routing can also guarantee the minimum delivery latency from each source to the sink. Performance improvements of up to fold and fold are observed in terms of routing traffic load reduction and energy efficiency, respectively, as compared to existing schemes [22]. Operating systems[edit] Operating systems for wireless sensor network nodes are typically less complex than general-purpose operating systems. They more strongly resemble embedded systems , for two reasons. First, wireless sensor networks are typically deployed with a particular application in mind, rather than as a general platform. Second, a need for low costs and low power leads most wireless sensor nodes to have low-power microcontrollers ensuring that mechanisms such as virtual memory are either unnecessary or too expensive to implement. However, such operating systems are often designed with real-time properties. TinyOS is perhaps the first [23] operating system specifically designed for wireless sensor networks. TinyOS is based on an event-driven programming model instead of multithreading. TinyOS programs are composed of event handlers and tasks with run-to-completion semantics. When an external event occurs, such as an incoming data packet or a sensor reading, TinyOS signals the appropriate event handler to handle the event. Event handlers can post tasks that are scheduled by the TinyOS kernel some time later. Online collaborative sensor data management platforms[edit] Online collaborative sensor data management platforms are on-line database services that allow sensor owners to register and connect their devices to feed data into an online database for storage and also allow developers to connect to the database and build their own applications based on that data. Examples include Xively and the Wikisensing platform. Such platforms simplify online collaboration between users over diverse data sets ranging from energy and environment data to that collected from transport services. The architecture of the Wikisensing system [25] describes the key components of such systems to include APIs and interfaces for online collaborators, a middleware containing the business logic

needed for the sensor data management and processing and a storage model suitable for the efficient storage and retrieval of large volumes of data. Simulation[edit] At present, agent-based modeling and simulation is the only paradigm which allows the simulation of complex behavior in the environments of wireless sensors such as flocking. Agent-based modelling was originally based on social simulation. Security[edit] Infrastructure-less architecture i. Therefore, security is a big concern when WSNs are deployed for special applications such as military and healthcare. Owing to their unique characteristics, traditional security methods of computer networks would be useless or less effective for WSNs. Hence, lack of security mechanisms would cause intrusions towards those networks. These intrusions need to be detected and mitigation methods should be applied. More interested readers would refer to Butun et al. Distributed sensor network[edit] If a centralized architecture is used in a sensor network and the central node fails, then the entire network will collapse, however the reliability of the sensor network can be increased by using a distributed control architecture. Distributed control is used in WSNs for the following reasons: Sensor nodes are prone to failure, For better collection of data, To provide nodes with backup in case of failure of the central node. There is also no centralised body to allocate the resources and they have to be self organized. Data integration and sensor web[edit] The data gathered from wireless sensor networks is usually saved in the form of numerical data in a central base station. Additionally, the Open Geospatial Consortium OGC is specifying standards for interoperability interfaces and metadata encodings that enable real time integration of heterogeneous sensor webs into the Internet, allowing any individual to monitor or control wireless sensor networks through a web browser. As nodes can inspect the data they forward, they can measure averages or directionality for example of readings from other nodes. For example, in sensing and monitoring applications, it is generally the case that neighboring sensor nodes monitoring an environmental feature typically register similar values. This kind of data redundancy due to the spatial correlation between sensor observations inspires techniques for in-network data aggregation and mining. Aggregation reduces the amount of network traffic which helps to reduce energy consumption on sensor nodes. Aggregation complicates the already existing security challenges for wireless sensor networks [30] and requires new security techniques tailored specifically for this scenario. Providing security to aggregate data in wireless sensor networks is known as secure data aggregation in WSN. Two main security challenges in secure data aggregation are confidentiality and integrity of data. While encryption is traditionally used to provide end to end confidentiality in wireless sensor network, the aggregators in a secure data aggregation scenario need to decrypt the encrypted data to perform aggregation. This exposes the plaintext at the aggregators, making the data vulnerable to attacks from an adversary. Similarly an aggregator can inject false data into the aggregate and make the base station accept false data. Thus, while data aggregation improves energy efficiency of a network, it complicates the existing security challenges.

3: Wireless sensor network - Wikipedia

text provides thorough coverage of wireless sensor networks, including applica- tions, communication and networking protocols, middleware, security, and manage- ment.

4: Wireless Sensor Network Topologies | Sensors Magazine

Examines issues of multimedia networks, registration, control of cameras (in simulations and real networks), localization and bounds on tracking Discusses system aspects of video networks, with chapters on providing testbed environments, data collection on activities, new integrated sensors for airborne sensors, face recognition, and building.

PT. 4. WIRELESS VIDEO SENSOR NETWORKS, COMMUNICATIONS AND CONTROL pdf

A modern introduction to probability and statistics The Well-Being of Pets and Companions San francisco lonely planet PSYCHIC ACAD BOX V2 (Psychic Academy) Life insurance in Malaysia Guide to oral history collections in Canada General frameworks for Caribbean prehistory Fidic yellow book 1999 Fischer v. Spassky: the World Chess Championship 1972 From nationwide competition to coast-to-coast monopoly Contents: The merry men Will o the mill Markheim Thrawn Janet Olalla The treasure of Franchard The waif w Transgenic crops and their applications for sustainable agriculture and food security Paul Christou and T Confessions of a Real Estate and Automotive Sales Blabbermouth Heat exchangers selection rating and thermal design third edition Writing as Political and Creative Expression U.S. Army Corps of Engineers Exponent laws worksheet grade 9 Semiconductor Thermal Measurement and Management Symposium (Semi-Therm) Production engineering questions and answers AutoCAD Release 13 Certification Exam Prep Manual Resemblance Nominalism The Temptation of the flesh The education of Karl Witte Climbing the political ladder Oscar: an inquiry into the nature of sanity Campo Aleman, the first ten years of Anaheim Michelin Red Guide 2005 Great Britain Ireland A parents guide to adolescents With the wild flowers from pussy-willow to thistledown Prelude to air from water Introduction: policymaking and intelligence on Iraq James P. Pfiffner and Mark Phythian Authoritarian specter Expert opinion : an employment lawyer on the record. Implementing Primary Health Care 2008 labour law survey Promoting reading with reading programs Moral panic over juvenile delinquency and the consequences Anaconda: 2 March 2002 Skyhooks-riding the crest of the industrial revolution The Tyranny of Relativism