Security features used for heterogeneous networks in wireless architecture

ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print) IJCST Vol. 3, ISSue 1, Jan. – MarCh 2012 Security Features used for Heterogeneous Networks in Wireless Architecture 1 Arshi Shamsi, 2Saoud Sarwar, 3Shamim Ahmad, 4Shahroukh Khan 2 IIMT Engineering College, Meerut, UP, India Al-Falah School of Engineering & Technology 3 Integral University, Lucknow, UP, India 4 APTECH, New Delhi, India 1 Abstract The ever-increasing demand of users for various wireless communication services has lead to the development and to the coexistence of different, and often incompatible, wireless networks.

Each one of these wireless networks has its own unique application and characteristics, as compared to other networks. Moreover, each network continues to evolve individually, most frequently not in a coordinated manner with other networks, further reducing compatibility among these networks. An integrated security mechanism is one of the key challenges in the Open Wireless network Architecture (OWA) because of the diversity of the wireless networks in OWA and the unique security mechanism used in each one of these networks.

The overall security of the network is as strong as its weakest component; integration of the overall security mechanism in OWA is of primary importance. In this paper, we comparatively analyze the unique network-centric features and security mechanisms of various heterogeneous wireless networks that are expected to be a part of OWA. Keywords Wireless Architecture, OWA, Security, Heterogeneous Networks I. Introduction The ever-increasing demand of users for various wireless communication services has lead to the development and to the coexistence of different, and often incompatible, wireless networks.

Each one of these wireless networks has its own unique application and characteristics, as compared to other networks. Moreover, each network continues to evolve individually, most frequently not in a coordinated manner with other networks, further reducing compatibility among these networks. From the user’s perspective, the future networks will implement Personal Service Mobility (PSM)—supporting ubiquitous and consistent access to the networks and preserving the user interfaces to network services, independent of the location of the user, including when the user roams across different networks.

From the perspective of the network, the realization of PSM will be accomplished through the integration of the various different wireless networks by the Open Wireless network Architecture (OWA). We term such individual networks OWA-related wireless networks. A. Network Integration Model The ever-increasing demand of users for various wireless communication services has lead to the development and to the co-existence of different, and often incompatible, wireless networks. Each one of these wireless networks has its own unique application and characteristics, as compared to other networks.

Moreover, each network continues to evolve individually, most frequently not in a coordinated manner with other networks. The integration of the various different wireless networks by the Open Wireless network Architecture (OWA) are termed individually as www. ijcst. com OWA-related wireless networks. We classify a network-centric integration model as either a tightly-coupled or a loosely-coupled model. In the tightly-coupled model, a network connects to another network as an alternative radio-access network. In a loosely coupled model the RNC of two wireless networks are independent and separated from each other.

Therefore, gateway functionality between the two RNC is required. To integrate several OWA-related wireless networks into a single architecture, there are a number of challenges that must be addressed; these include support for mobility management, Quality of Service (QoS) provisioning, and security interoperability. Especially, integration of security techniques used by these various and different networks is one of the key problems, as due to the inherent vulnerability of wireless communications, the security requirements of wireless communication are usually more stringent than in wired networks.

Also, because of the inherent and often quite fundamental differences among the various OWArelated wireless networks, integration of the security schemes of those networks is not an easy task. Fig. 1: An Instance of Tightly Intgrated Network Model Amongthe Five Wirless Network In the following section, we discuss some of those differences [1]. 1. Architectural Characteristics Basic characteristics, such as device capacity, radio bandwidth, coverage area, maximal transmission power, and other architectural features can significantly differ among the OWA-related wireless networks.

For example, from an architectural point of view, cellular networks and WLAN (wireless local area networks), which are both infrastructure-based networks, can use infrastructure-aided security, such as an Access point (AP) or a Base Station (BS), to perform some security functions. In contrast, infrastructure-less Ad-Hoc and sensor networks must rely only on network nodes for execution of the security functions. 2. Security Requirements The security requirements of network communication services are tailored to the special requirements of the applications and the capabilities of a network.

In general, security requirements InternatIonal Journal of Computer SCIenCe and teChnology 407 IJCST Vol. 3, ISSue 1, Jan. – MarCh 2012 ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print) depend on the vulnerability of the Communicated data. The implementation of those security requirements must match the available network services. 3. Selected Security Mechanisms and Standards The designers of each network adopted a particular set of security mechanisms and standards, which in general, may not be compatible with those of the other OWA related wireless networks.

Those security mechanisms include key distribution methods, cryptographic procedures, and crypto algorithms. Often the security mechanisms are so different that integration of those mechanisms is impossible. To realize ISA (Industry Standard Architecture) in OWA, security operations should be independent from the specific characteristics of the OWA-related wireless networks. Therefore, we focus on a security management approach, which would co-operate with the individual security mechanisms of the networks, rather than designing a single security mechanism to be used hroughout all the networks. We consider Ad-Hoc networks, sensor networks, and RFID (radio frequency identification) systems, as well as WLAN and cellular networks as OWA-related wireless networks and compares the security services of the individual wireless networks. II. Overview of Security Technologies We discuss cryptographic mechanisms, hash schemes, and key management methods here. [8] A cryptographic mechanism, a scheme that is controlled by a cryptographic key, is composed of two processes: encryption and decryption. The most common cryptographic mechanisms are: A.

Private-key (or symmetric) Cryptosystem A cryptographic mechanism where the same key is used for both the encryption and the decryption processes. B. Public-key (or asymmetric) Cryptosystem A cryptographic mechanism where different keys are used for encryption and decryption A hash mechanism is a deterministic function that maps a bit string of an arbitrary length to a value (hash value) that is a bit string of a fixed (usually smaller) length. Hash mechanisms are used in cryptography as a method to generate message digests for digital signature, practical pseudo-random numbers, and for data integrity.

Key management is a method for establishing and renewing keys to communicating parties. A key for a symmetric cryptosystem can be established mainly by two methods: conventional techniques and public-key techniques. In the conventional techniques, a physically secure means is employed to make the communicating parties exclusively share a key. In the public-key techniques, public-key cryptosystem protocols are used to establish a symmetric session key at the communicating parties. III.

Security Mechanisms of the OWA Networks We compare the unique security mechanisms of the individual OWA-related wireless networks, focusing on the distinguishable security features of each of these networks. A. Security of Cellular Networks We summarize the 3G UMTS security mechanism as an example of security mechanisms used in cellular networks. The service coverage area of UMTS can be divided into Radio Access Network (RAN) and Core Networks (CN), with each of the two areas having its own unique security mechanisms. The security mechanisms of RAN consist of the following four functions [3]: 1.

User privacy is based on temporary identities such as pseudonyms or on re-authentication identities that are generated by an Authentication, Accounting, and Authorization (AAA) server. 2. Mutual authentication is based on the challenge handshake authentication protocol (CHAP) of a single round-trip exchange with a pre-established key, K. 3. Session key agreement, which occurs during a mutual authentication process, generates session keys for Confidentiality (CK), and for Integrity (IK), based on the random challenge, RAND. 4.

Secure communication with a session key enables confidential communication and message integrity; in the 3GPP, the KASUMI [4] algorithm is recommended, which is a 64-byte block encryption algorithm, used for the f8 function. The goal of Network Domain Security (NDS) is to secure all important control plane protocols. B. WLAN Security The security of WLAN can be divided into authentication and confidentiality features. The original IEEE 802. 11 standard supports the confidentiality feature through

Wired Equivalent Privacy (WEP) and entity authentication through open-system [7].

However, WLAN security proved to be vulnerable due to collision of the Initial Vector (IV) and due to its short key length. To address these security faults of IEEE 802. 11, the IEEE 802. 11i standard was proposed and includes [4]: 1. Authentication 802. 11i does not use the shared-key-based approach of the 802. 11 standards for authentication and for key management. Instead, it interoperates with 802. 11X, which uses a port-based mechanism for authentication and device authorization. 2. Confidentiality To address the weaknesses of WEP, IEEE 802. 1i developed the Temporary Key Integrity Protocol (TKIP). TKIP also is based on the RC4 encryption, which is the most widely-used stream cipher, to generate key stream. TKIP defines a Temporal Key (TK), which is a 128-bit shared secret key, extends the 24-bit IV to 48-bit length, and employs a packet sequence counter to protect against replay attack. Nevertheless, because TKIP uses the RC4 stream algorithm, it cannot overcome the cryptographic limitation of RC4. As a long-term solution, IEEE 802. 11i also defines the Counter mode with CBC/MAC3 protocol (CCMP) to replace WEP.

CCMP uses the Advanced Encryption Standard (AES), which adopts the CCM mode with 128-bit keys and 128bit block size operation. C. Security of Ad-Hoc Networks The efforts to design security mechanisms for Ad-Hoc networks concentrated mainly on supporting security for the routing operation of Ad-Hoc protocols. The secure routing protocols rely on the availability of secure key distribution schemes [5]. 1. Key Distribution Because of the infrastructure less and the open-environment attributes of

Ad-Hoc networks, a public-key pproach, based on the threshold schemes, is a more applicable approach than w w w. i j c s t. c o m 408 InternatIonal Journal of Computer SCIenCe and teChnology ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print) IJCST Vol. 3, ISSue 1, Jan. – MarCh 2012 private-key schemes [8], although a private-key scheme also can be used. The public-key distribution schemes of Ad-Hoc networks can be classified into three mechanisms: partial distribution, full distribution, and self-organized. In the partial distribution method, n Ad-Hoc nodes are delegated as server nodes [8].

Each of these server nodes can generate a partial signature, using its share of the certificate singing key; however, only by the commitment of t such partial signatures can a valid certificate be obtained. In the full distribution method, each neighbor node possesses a portion of the signature key of CA, 4 which is restored by a combination of at least k pieces of partial secret keys. The main difference between the two distribution methods is that the full distribution method does not designate specific nodes such as server nodes, and it uses a combination of any network nodes.

In the self-organized method, each node generates its own certificate and constructs certificate chains with one-hop-away nodes until reaching the destination node. 2. Secure Routing Protocols We divide secure routing protocols into public key-based and private key-based protocols, according to their underlying cryptographic algorithms. The representative private key-based protocol is the Secure Routing Protocol (SRP)[7]. SRP assumes the existence of security associations between the source node and the destination node only.

SRP can provide message authentication of the route request and the route reply messages. A typical public key based scheme is the secure AODV, SAODV protocol. SAODV enhances the confidentiality and the authentication functions of the original AODV protocol by the digital signature scheme and by the hop-count hashing mechanism. A source node sends a route request message after signing it with its private key. Then, intermediate nodes verify the signed route request message and re-sign it after adding new information. D.

Security of Sensor Networks Security requirements of sensor networks are similar to those of Ad-Hoc networks, as network features are similar to those of AdHoc networks. However, because the capabilities of sensor nodes are too limited to operate a public-key mechanism, the private keybased cryptosystem is more applicable. In particular, the closedenvironment feature of sensor networks makes it possible to predeploy information within the devices during the manufacturing stage, information that could be used to generate common session keys during the network operation.

Therefore, a sensor network can use the Pre-deployed Key Distribution (PKD) scheme as a session key distribution scheme. E. RFID Security Because the main application of an RFID system is to convey a particular type of information to the RFID reader through an automatic identification process of a person or an object, the security concerns of an RFID system are focused on the privacy of ID information during wireless transmission between a tag and a reader. We divide security schemes for an RFID system into the following three categories. 1.

Non-Cryptographic Schemes The representative non-cryptographic mechanisms use the kill command and blocker tag. To kill tags, a reader must transmit a tag-specific 32-bit PIN, which is to prevent wanton deactivation of tags. If a tag receives the kill command, it remains permanently in the inactive mode. A blocker tag is a special RFID tag that w w w. i j c s t. c o m prevents unwanted scanning of tags. Through the blocker tag, the information of a tag becomes permanently or temporarily inactive at an optional location and for an optional time period. 2.

Lightweight Cryptographic Schemes The representative lightweight cryptographic mechanisms use a pseudonym or apply a one-way hash chain scheme. Juels, et al. [9], proposed a minimalist system where every tag contains a small collection of pseudonyms, and where it rotates through them and releases a different one on each reader query. An authorized reader can store the full pseudonym set for a tag in advance and therefore identify the tag consistently. In the case of a one-way hash chain scheme, the tag transmits the hash chain value of its ID on the air, rather han its real ID. Because the reader already has the hash-chain information, it can find the corresponding ID and identify the tag. 3. Conventional Cryptographic Schemes In this an RFID tag includes the encrypted ID, public key, and private key that are used for encryption and decryption and that also are stored in a law enforcement agency. IV. Fundamental Security Approaches In the following section, we summarize the possible approaches for a security integration scheme of OWN and consider the unique features of each heterogeneous wireless network [1]. . Multiple Security Mechanisms for Source-toDestination Security Although a single underlying cryptographic algorithm as a security mechanism is best from the integration point of view, nevertheless, a single security mechanism cannot guarantee the particular security requirements of each one of the OWN networks. 2. Evolution from the Notion of Security Mechanisms to the Notion of Security Management To support multiple security mechanisms, an efficient interoperation procedure among the mechanisms is required.

In other words, the key issue of integrated OWN security is the design of an appropriate security management procedure, rather than a single optimal security mechanism. 3. Upper Layer Security Approach As multiple security mechanisms will co-exist within OWN, the individual security mechanisms will continue to be used within a single network domain. Thus, for transparent security management, ISA must be implemented in an upper layer of the protocol stack; that is, at the network layer or above. . Mutually Independent Security Processes The ongoing security interoperation, for example, between a WLAN and a cellular network, is a cellular network-based operation, as the security mechanism of cellular networks is more stable than that of WLAN. However, it is expected that the individual security mechanisms of each network will continue to be improved and adapted to the particular security requirements of the network. Furthermore, OWN will be managed by multiple operators.

Therefore, ISA cannot delegate more responsibility to a specific network domain, as the authority to provide security for each one of the wireless networks cannot rely on elements of other networks. InternatIonal Journal of Computer SCIenCe and teChnology 409 IJCST Vol. 3, ISSue 1, Jan. – MarCh 2012 ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print) V. Conclusion As indicated by this paper, the security concerns are one of the toughest challenges in successful realization of OWA. Our work summarizes a brief description of various security mechanisms available.

The designers of each network adopted a particular set of security mechanisms and standards, which in general, may not be compatible with those of the other OWA related wireless networks. To realize ISA (Industry Standard Architecture) in OWA, security operations should be independent from the specific characteristics of the OWA-related wireless networks.

References [1] W. W. Lu,“ Open Wireless Architecture and Its Enhanced Performance”, IEEE Commun. Mag. , Vol. 41, No. 6, June 2003, pp. 106–07. [2] A. Shamir,“ Identity-Based Cryptosystems and Signature Schemes”, Proc. CRYPTO ’84, LNCS196, Springer-Verlag, 1985, pp. 48–53. [3] G. M. Koien,“ An Introduction to Access Security in UMTS,” IEEE Wireless Commun. , Vol. 11, No. 1, Feb. 2004, pp. 8–18. [4] J. C. Chen, M. C. Jiang, Y. W. Liu,“ Wireless LAN Security and IEEE802. 11i,” IEEE Wireless Commun. , Vol. 12, No. 1, Feb. 2005, pp. 27–36. [5] L. Zhou, Z. J. Haas,“ Securing Ad-Hoc Networks,“ IEEE Network, Vol. 13, No. 6, Nov. /Dec. 1999. [6] P. Papadimitratos, Z. J. Haas,“ Secure Routing for Mobile Ad-Hoc Networks”, Proc. SCS Commun. Networks and Distrib. Sys. Modeling and Simulation Conf. , Jan. 2002, pp. 7–31. [7] M. G. Zapata,“ Secure Ad-Hoc On-Demand Distance Vector Routing”, ACM Mobile Comp. Commun. Rev. , Vol. 6, No. 3, July 2002, pp. 106-07. [8] A. Juels et al. ,“ Minimalist Cryptography for Low-Cost RFID Tags”, Proc. 4th Int’l. Conf. Security in Commun. Networks, LNCS 3352, Springer-Verlag, 2004, pp-149-64. [9] Bok Yong Choi, Deok Gyu Lee,“ RHDP-Scheme for RFID’s Efficiency Improvement on the Ubiquitous Computing”, SpringerLink,

Vol. 344/2006, 4, Oct 2006, pp. 1068-1077. Arshi Shamsi received his B. Tech. degree in computer science from Vira College of Engineering,(from U. P. T. U.

Lucknow) Bijnor, India, in 2004 and pursuing M. Tech. degree in Computer Science from Al-Falah School of Engineering and Technology,(Maharishi Dayanand University, Rohtak) Haryana. He is working as Assistant Professor, with Department of Computer Science, at IIMT Engineering College. He is having a total work experience of 7 years. Shahroukh Khan received his B. Tech. degree in computer science & Engg from Shri Ram Murti Smarak College of Engineering & Technology, Bareilly, India, in 2007 and pursuing M. Tech(CSE) Degree in Computer Science from Al-Falah School of Engineering & Technology (M.

D. University, Rohtak, Haryana). He is working as Lecturer, with Department of Computer Science & Engineering, at Integral University, Lucknow. He is having a total work experience of 4. 5 years. Shamim Ahmad received his B. E. degree in Computer Engg from Faculty of Engg. & Technology, Jamia Millia Islamia(Central University), India, in 2009 and pursuing M. Tech. Degree in Computer Science Engg. from Alfalah School of Engg. & Technology, Faridabad (affliated to Maharishi Dayanand University, Rohtak, Haryana). He is working as Software Trainer, with Aptech Ltd.

He is having a total work Saoud Sarwar received his M. Tech (IT) from Allahabad Agriculture University in 2004. Currently he is pursuing Ph. D from Bhagwant University, Ajmer (Rajasthan). He is working as Head of department in Al-Falah School of Engineering & Technology. He is also working as M. Tech (CSE) coordinator. He is having experience of more than 7 years. He has published numerous research papers in National & International Conferences. experience of 2 years. 410 InternatIonal Journal of Computer SCIenCe and teChnology www.ijcst.com