International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 4 Issue 6, June-2015, pp: (164-166), Impact Factor: 1.252, Available online at: www.erpublications.com

Survey for Identity Based Public Key to Improve Wireless Sensor Network Security

Komal Sangwan[1], Dr. Yudhvir singh[2]*
[1,2]University Institute of Engineering and Technology, Maharshi Dayanand University, Rohtak, India

Abstract: In wsn security, we examined how many of the wireless access points detected were secured with some form of encryption, excluding hotspots. RSA officials said the 2008 results show some dramatic improvements in security practice key algorithms are tractable on mote-class hardware and can achieve message confidentiality. However, key distribution and management remains a significant practical challenge, and these algorithms poorly support message authenticity and integrity. In our study we reviewed, Public Key Cryptography (PKC) is widely used to support symmetric key management, as well as message authenticity and integrity. proposed techniques that simplify brute-forcing RSA, and other work based on suggests that 1024-bit RSA keys can be broken in one year by a device that costs $10 million rather than trillions as in previous predictions. It is currently recommended to use an RSA key at least 2048 bit long. Therefore, the default RSA key size in sec Fleck is 2048 bits.

Keywords: Identity Based-RSA , RSA, PKC, Security , WSN, PKM , Encryption , AODV.

1. INTRODUCTION

The survey also examined how many of the wireless access points detected were secured with some form of encryption, excluding hotspots. RSA officials said the 2008 results show some dramatic improvements in security practice. In New York City, 97 percent of corporate access points had encryption in place - up from 76 percent last year. The results are the best in the survey's history, said RSA. In Paris, 94 percent of corporate access points were encrypted. London still has 20 percent of all business access points unprotected by any form of wireless encryption. Now that Wired Equivalent Privacy (WEP), the original wireless encryption standard, is discredited, "the 2008 survey paid close attention to the types of encryption in-play, and the relative adoption of more advanced forms of wireless encryption, including Wi-Fi Protected Access (WPA) or WPA2," RSA said in the statement. "Overall, the adoption of non-WEP advanced encryption is encouraging."

1.1. Cryptography in WSN

Cryptography is basically the conversion of data into a secret code for transmission over a public network. Today's cryptography is more than encryption and decryption. Cryptography is the study of “mathematical” systems for solving two kinds of security problems: privacy and authentication [3].

1.1.1. Private Key Cryptography

A single key is used for both encryption and decryption. Encryption the data is encrypted by any encryption algorithm using the key. Only the user having the access to the same ‘key’ can decrypt the encrypted data. Examples are AES, 3DES etc.

1.1.2. Public Key Cryptography

In public key cryptography each user or the device taking part in the communication have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations . Only the particular device knows the private key whereas the public key is distributed to all devices taking part in the communication. Paris lead the way in non-WEP security, with 72 percent of access points (excluding public hotspots) found to be using advanced security. New York City and London were more modest at 49 percent and 48 percent respectively. A majority of wireless access points relied on either on WEP or used no encryption at all, according to the survey. We will also discuss some RSA terms and parameters, such

as modulus (n), random numbers (p and q), public exponents (e) and key sizes (k), and their implications to the RSA algorithm computation complexity and security levels.

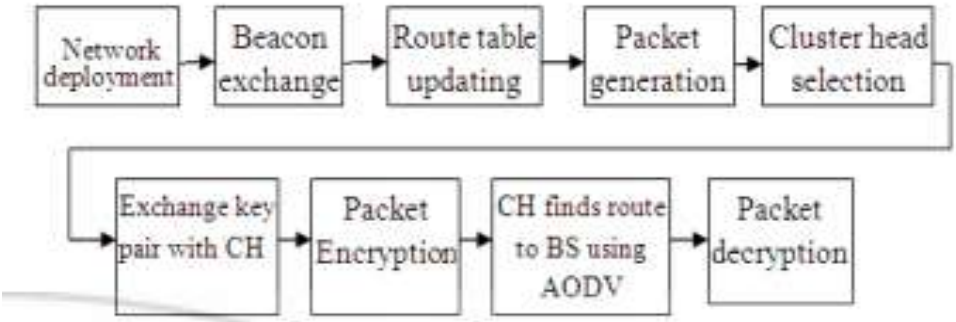

Figure 1: Block Diagram for WSN KE Concept

In Above figure , RSA is an algorithm for public key cryptography (PKC), also called asymmetric cryptography, in which the encryption key is different to the decryption key. RSA is the first algorithm that is suitable for signing and encryption, and is used widely in secure communication protocols, such as Secure Shell (SSH) and Secure Sockets Layer (SSL), in the Internet. Symmetric keys are typically generated by a pseudo-random number generator in previous work [14].

Security in WSN

Wireless networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected.

1.1 Wireless Sensor Network

Security Challenges Because sensor networks pose unique challenges, traditional security techniques used in traditional networks cannot be applied directly. First, to make sensor networks economically profitable as sensor devices are limited in their energy, computation, and communication capabilities. Second, sensor nodes are often deployed in accessible areas, presenting the added risk of physical attack [2].

Data Confidentiality: Confidentiality means keeping information secret from unauthorized parties. A sensor network should not leak sensor readings to neighboring networks.

Data Authenticity and Integrity: One can easily inject malicious data in sensor network. So receiver should make sure that data it received is correct and legitimate data as in this malicious data can lead to wrong interpretation by receiver

Data Cleanness: Data freshness implies that the data is recent, and it ensures no old messages are replayed over network. For this counter must be used that can determine freshness. Availability: Availability ensures that services and information can be accessed at the time they are required.

2. RELATED WORK

In [2] proposed main aspects of wireless sensor network security into four major categories: the obstacles to sensor network security, the requirements of a secure wireless sensor network, attacks, and defensive measures. The organization then follows this classification. They provide both a general overview of the rather broad area of wireless sensor network security. In [3] proposed time and power consumption of public key cryptography algorithm for signature and key management by simulation. Cryptographic algorithm for authentication and encryption can be implemented in two ways: using public keys or private keys. Here Sensor nodes must be reconfigured, calibrated, and reprogrammed. Such operations are very sensible to possible attacks. Finally, it must be mentioned that they ignore the problem of key management. In [4] proposed several schemes to secure communications in WSNs. These schemes are classified into three classifications based on the cryptographic techniques: symmetric keys, asymmetric keys and one-way hashing functions. There are different classifications based on the application scenarios, including: deployment, organization, re-keying, cryptography and

authentication and are also described critical success factors of wireless sensor networks, those are soft message encryption, multiple communication paths, efficient data aggregation, malicious node detection, node revocation-awareness.
In [5] proposed Current state-of-the-art protocols and algorithms for securing internet communication. By using a security protocols will make the sensor network a more attractive option.

3. DISCUSSION

This discussion routing protocols is used in wireless sensor networks, so it is not possible to provide a single security protocol that will be able to secure each type of routing protocol. Before introducing several techniques used to provide secure routing in wireless sensor networks, we will begin with a general overview of several routing protocols that are currently in use. An excellent discussion on many of the attacks on routing protocols is also discussed in [40]. In general, packet routing algorithms are used to exchange messages with sensor nodes that are outside of a particular radio range. This is different than to sensors that are within radio range where packets can be transmitted using a single hop. In such single hop networks security is still a concern, but is more accurately addressed through secure broadcasting and multicasting. The first packet routing algorithm is based on node identifiers similar to traditional routing. In this case, each sensor is identified by an address and routing to/from the sensor is based on the address. This is generally considered inefficient in sensor networks, where nodes are expected to be addressed by their location, rather than their identifier

4. CONCLUSION

In this paper, we observed that in the proposed model the energy consumption using RSA security protocol is quite optimistic. Here we have increased the number of nodes and compare the parameters and remaining of nodes, PDR have been increased and Throughput, control overhead are decreased, because in present system technique used is routing non cluster and in proposed routing CH is used. By using routing CH we decreased number of encryption and decryption to reduce the energy consumption

REFREENCES

[1]. John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary, “Wireless Sensor Network Security: A Survey”, Security in Distributed, Grid and Pervasive Computing 17:367-388, 2009.
[2]. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless sensor networks: A survey, Computer Networks 38(4) (2002) 393–422.
[3]. Crossbow Technology Incorporation.
[4]. D. Boyle, T. Newe, “Security Protocols for use with Wireless Sensor Networks: A Survey of Security Architectures”, Proceedings of the Third International Conference on Wireless and Mobile Communications, 2010.
[5]. R.A Sheikh, Sung young Lee, Mohammad A. U. Khan,and Young Jae Song, “LSec: Lightweight Secure Protocol for Distributed Wireless Sensor Network”, IFIP International Federation for Information Processing 2006.
[6]. D. W. Carman, P. S. Krus, and B. J. Matt. “Constraints and approaches for distributed sensor network security. Technical Report”, 00-010, NAI Labs, Network Associates Inc., Glenwood, MD, 2000.