International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.4., 2015
(July-Aug)

REVIEW ARTICLE

ISSN: 2321-7758

PROVIDING SECURITY IN SENSOR NETWORKS APPLICATION OF DIGITAL SIGNATURE ALGORITHM

HARMANJOT KAUR, HARTEJ SINGH
Department of ECE
Global Institutes Amritsar

ISSN:2321-7758
International Journal of Engineering Research-Online
A peer reviewed, open access international scientific journal
www.ijoer.in

ABSTRACT

Networking is the backbone of today's communication world. Wireless sensor networks are an important part of distributed networks. They are innovative, autonomous networking devices that consume low-power, have low-cost and are small-sized devices. They create networking infrastructure which is less ad-hoc. The information is collected and communicated using sensors. Wireless sensor devices are used in many application areas Line all networks, security is a vital context for such networks also. Security goals like confidentiality, integrity, data origin authentication, access control and availability are set. The traditional approaches that are applied to prevent the attacks on wireless networks include Digital Signature Algorithms use Authentication for providing security. RSA with 512 bit key length is used for encryption and decryption data. Even breaking into this level of security is not easy. As these devices have low computation power, small memory and battery power, very complex algorithms cannot be used.

In order to enhance the network security and make the communication more secure, RSA with 1024-bit keys (RSA-1024) is the accepted level of security currently. RSA with 2048-bit key length and 4096-bit key length has been used to enhance the communication security.

Keywords: Encryption, Decryption, RSA, WSN, Secret Key Cryptography (SKC).

1. INTRODUCTION

The present work is aimed at to provide network security for the data communication over the wireless network using the asymmetric approach of cryptography. The use of network security is to protect the network information and resources from the unauthorized access. All the application that are based on computer networking and deals with data communication over the network require network security. As in the case of wireless sensor networks, various constraints to security level provided include low computation capability, small memory, limited energy resources [3], susceptibility to physical capture, lack of infrastructure. These issues put security challenges and require making innovative approaches desirable.

Major security threats are the attacks like DoS (Denial of Service) Attack, Node Clone Attack and Sybil attack etc. Security plays a fundamental role in many wireless network applications. In the wireless nodes, batteries are the source of energy. So, while providing security using existing security mechanisms are inadequate because energy consumption becomes a key consideration. and new approaches are desired.

For providing security in data communication, cryptography is used to secure the data packets. The data is encrypted at the transmission and decrypted back at the receiver end. Today, various cryptography techniques and algorithms exist but these cryptography algorithms are complex, slow and power hungry. They require more processing power because of high computations involved which make them impractical for the wireless network nodes.

2. CRYPTOGRAPHIC ALGORITHMS

Based on the number of keys involved in the encryption and decryption process, there are three types of algorithms that are employed[7], and further defined by their application and use.

- Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption
- Public Key Cryptography (PKC): Uses one key for encryption and another for decryption
- Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information

Cryptography has four basic goals known as Confidentiality, Integrity, Authentication and No repudiation.

2.1 Symmetric Cryptography Algorithms:

- Data Encryption Standard (DES)
- Triple DES (3DES),
- International Data Encryption Algorithm (IDEA),
- Blowfish
- Skipjack,
- Advanced Encryption
- Standard (AES).

Limitations of Symmetric Algorithms include[6]:

1. Distribution of the key is the problem, because once the key is compromised, it means a total security leak.
2. It does not provide No repudiation of data.
3. Once a member of a security group leaves a new key must be generated and distributed.

2.2 Asymmetric Key Algorithms

It is the public key algorithm that covers up all the weakness found in symmetric key system. This algorithm uses two keys - public and private which are used for data encryption and data decryption. One of the keys is the Public key that is shared to all whereas each member of the group had his own private key, which is private to him and only known to him. Few asymmetric algorithms Diffie-Hellman, RSA, Digital Signature Algorithm (DSA), Elliptic Curve Cryptography(ECC) are currently in use. The most commonly used asymmetric algorithm is the RSA algorithm.

2.3 Hashing Algorithms

Hashing algorithms are secure one and are used with digital signatures, it provides a fixed length digital digest of a message and it is almost impossible to derive a message from its hash function. From the security point of view, it is also very much unlikely that the same two messages will generate the same hash function-thus a very effective way to ensure integrity of a message. Most commonly used hash algorithms are: Message Digest 2 (MD2), Message Digest 4 (MD4), Message Digest 5 (MD5), Secure Hash Algorithm (SHA), Hash-Based Message Authentication Code (HMAC).

2.4 New Directions :RSA Algorithm

The popular RSA algorithm invented in 1977 is named after Ron Rivest, Adi Shamir and Len Adleman[11]. Although the basic technique was first discovered in 1973 by Clifford Cocks of CESG (part of the British GCHQ) but this was a secret until 1997 and also, the patent taken out by RSA Labs has expired. The RSA algorithm can be used for both public key encryption and digital signatures. The security is based on the difficulty of factoring large integers in the algorithm.

3. Related Work

Based upon the work done and the experience of network and wireless security experts with factoring large numbers and studying the key length of the public key algorithms used, it was estimated that within three years, the algorithmic and computer technology used for network security that was based to factor RSA-512 bit key length will be widespread, at least in the scientific world, so that by then 512-bit RSA keys will certainly not be safe anymore. Something more secure is required and thus the security professionals were made to think about the solution to provide security. With unsafe network, the keys used for authentication or for the protection of data will be able to secure only for a small period longer than a few days[15].

Although 512-bit RSA keys protect approximately 95% of today's E-commerce on the Internet at least outside the USA and are used in SSL (Secure Socket Layer) handshake protocols. The complete E-commerce business in the world will be on the much larger number. Understanding the urgency of the undesirable situation, it became important to use "strong" cryptography like RSA. If we look at history in the past, on January 12, 2000, the U.S. Department of Commerce Bureau of Export Administration (BXA) issued new encryption export regulations which allow U.S. companies to use larger than 512-bit keys in RSA-based products. As a result, the work was done to enhance the security and use larger key length by replacing the 512-bit keys by 768-bit. This was thought that this will create the much more favorable conditions for secure internet communication.

Therefore, the related work in the cryptography and network security was up to key length 512 bit and then by 768-bit key. But it was too was unable to provide the required level of security. So the need to implement RSA-1024 bit becomes necessary to cope up with the upcoming needs for security[15]. Now, with enhancement in technology, RSA-2048 and RSA-4096 bit key length is the need of the hour which is used in the present work to see the viability and the security level in the wireless sensor network.

4. Key length

The key length of an RSA key, it is basically referring to the length of the modulus, *n*, in bit[10]. A key length of 768 bits or 1024 bits is now no longer considered secure. The longer the information is needed to be kept secure, the longer the key you should use. Keep up to date with the latest recommendations in the security journals.

RSA with 2048-bit keys (RSA-2048) and 4096-bit keys (RSA-4096) is implemented which provides a currently accepted level of security for many applications to protect data beyond the encryption of a 1024-bit block[12].

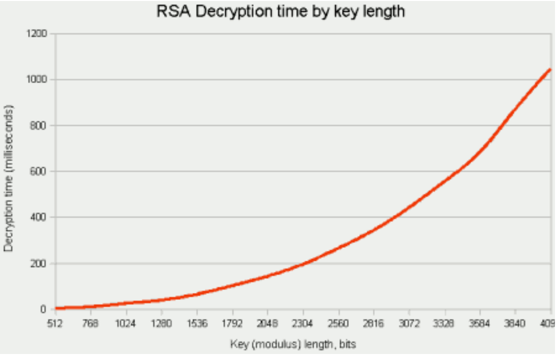

Figure 1: RSA decryption time by key length

With every doubling of the RSA key length, decryption is 6-7 times slower. So it requires much more time to decrypt the cipher text. Adi Shamir who was one of the RSA creators estimated that "Around 8.4 million CPU years are needed to factorize even a 1024-bit number in software". His estimate is specifically 8.4 million uniprocessor PCs, taking into account memory and data transfer requirements

But the estimated energy consumption is a much lower for RSA-1024 bit. Algorithm is more secure than the (RSA-768 bit) algorithm. RSA-1024 bit, when implemented consumed more power on same processor.

Similarly, when the key length is increased to 4096 bit, the energy consumption level is less than the 2048-bit key length on the same processor. This shows that the network can be made secure using the 4096-bit key length and will make the network more secure and will be nearly impossible to break into network security.

5. CONCLUSION

Cryptography is used to secure the communication data packets. It encrypts the data while transmitting it and decrypts it back at the receiver end. Today, various cryptography techniques and algorithms exist. Cryptography algorithms are complex, slow, power hungry. They involve high computations and require more processing power which makes them impractical for the wireless network nodes.

RSA with 4096-bit keys (RSA-4096) is able to secure the network communication data and is possible to implement in the wireless sensor nodes. It provides much secure level of level of security for many applications to protect data beyond the encryption of a 4096-bit block.

6. FUTURE SCOPE

Although research efforts have been made on cryptography, key management, secure routing, secure data aggregation, and intrusion detection in WSNs, there are still some challenges to be addressed. Firstly, the security mechanisms are highly application-specific so the selection of the appropriate cryptographic methods depends on the processing capability of sensor nodes. Secondly, sensors are characterized by the constraints on energy, computation capability, memory, and communication . bandwidth. The design of security services in WSNs must satisfy these constraints.

REFERENCES

[1]. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," in Third IEEE International Conference on Pervasive Computing and Communications (PERCOM'05). IEEE Computer Society Press, 2005, pp. 324-328.

[2]. Adrian Perrig, John Stankovic, and David Wagner. Security in wireless sensor networks. Commun.ACM, 47(6):53{57, 2004.

[3]. Agah, S. K. Das, K. Basu, and M. Asadi. Intrusion Detection in Sensor Networks: a Non-Cooperative Game Approach. In Proceedings of Third IEEE International Symposium on the Network Computing and Applications (NCA'04), pages 343 - 346. IEEE Computer Society, 2004.

[4]. Bekara and M. Laurent-Maknavicius. A New Protocol for Securing Wireless Sensor Networks against Nodes Replication Attacks. In Third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMOB 2007), pages 59-59, 2007.

[5]. Bertoni, L. Breveglieri, and M. Venturi. ECC Hardware Coprocessors for 8-bit Systems and Power Consumption Considerations. In Third International Conference on Information Technology: New Generations (ITNG 2006), pages 573-574, 20

[6]. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung. Perfectly-Secure Key Distribution for Dynamic Conferences. Information and Computation, 164(1):1-23, 1998.

[7]. Carman, B. Matt, D. Balenson, and P. Kruus, "A communications security architecture and cryptographic mechanisms for distributed sensor networks," in DARPA SensIT Workshop. NAI Labs, The Security Research Division Network Associates, Inc., 1999.[Online]. Available:

[8]. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in Proceedings of the 2003 IEEE Symposium on Security and Privacy. IEEE Computer Society, 2003.

[9]. D. Chakrabarti, S. Maitra, and B. Roy. A Key Pre-distribution Scheme for Wireless Sensor Networks: Merging Blocks in Combinatorial Design. In Information Security, pages 89- 103. LNCS 3650, 2005.

[10]. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," in Third IEEE International Conference on Pervasive Computing and Communications (PERCOM'05). IEEE Computer Society Press, 2005, pp. 324-328.

[11]. Adrian Perrig, John Stankovic, and David Wagner. Security in wireless sensor networks. Commun.ACM, 47(6):53{57, 2004.

[12]. Agah, S. K. Das, K. Basu, and M. Asadi. Intrusion Detection in Sensor Networks: a Non-Cooperative Game Approach. In Proceedings of Third IEEE International

Symposium on the Network Computing and Applications (NCA'04), pages 343 - 346. IEEE Computer Society, 2004.

[13]. Bekara and M. Laurent-Maknavicius. A New Protocol for Securing Wireless Sensor Networks against Nodes Replication Attacks. In Third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMOB 2007), pages 59-59, 2007.

[14]. Bertoni, L. Breveglieri, and M. Venturi. ECC Hardware Coprocessors for 8-bit Systems and Power Consumption Considerations. In Third International Conference on Information Technology: New Generations (ITNG 2006), pages 573-574, 20

[15]. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung. Perfectly-Secure Key Distribution for Dynamic Conferences. Information and Computation, 164(1):1-23, 1998.

[16]. Carman, B. Matt, D. Balenson, and P. Kruus, "A communications security architecture and cryptographic mechanisms for distributed sensor networks," in DARPA SensIT Workshop. NAI Labs, The Security Research Division Network Associates, Inc., 1999.

[17]. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in Proceedings of the 2003 IEEE Symposium on Security and Privacy. IEEE Computer Society, 2003.

[18]. D. Chakrabarti, S. Maitra, and B. Roy. A Key Pre-distribution Scheme for Wireless Sensor Networks: Merging Blocks in Combinatorial Design. In Information Security, pages 89- 103. LNCS 3650, 2005.

[19]. Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks," in SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems. New York, NY, USA: ACM Press, 2004, pp. 162-175.

[20]. Lin and G. Noubir, "Low Power DOS Attacks in Data Wireless LANs and Countermeasures," Northeastern University, Tech. Rep., 2002.

[21]. R. Anderson, H. Chan, and A. Perrig. Key Infection : Smart Trust for Smart Dust. In Proceedings of the 12th IEEE International Conference on Network Protocols (ICNP'04), pages 206-215, 2004.

[22]. R. Brooks, P. Y. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M. T. Kandemir. On the Detection of Clones in Sensor Networks Using Random Key Predistribution. IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, 37(6):1246-1258, 2007.

[23]. S. S. C¸amtepe and B. Yener. Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks. IEEE/ACM Transactions on Networking, 15(2):346-358, 2007.

[24]. Stefania Cavallar , "Factorization of a 512-bit RSA Modulus" CWI, P.O. Box 94079, 1090 GB Amsterdam, The Netherlands,

[25]. T. Arampatzis, J. Lygeros, and S. Manesis. A Survey of Applications of Wireless Sensors and Wireless Sensor Networks. In Proceedings of the 13th Mediterranean Conference on Control and Automation, pages 719-724, 2005.

[26]. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," IEEE Wireless Communications, vol. 11, no. 1, pp. 38-7, Feb. 2004.

[27]. Abdul D S, Elminaam, Kader H M A and Hadhoud "Performance Evaluation of Symmetric Encryption Algorithms," IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, December 2008.

[28]. Anjum F, Subhadrabandhu D and Sarkar "Signature based Intrusion Detection for

Wireless Ad-Hoc Networks: A Comparative study of various routing protocols", In IEEE 58th Vehicular Technology Conference,2004.

[29]. DhawanP"Performance Comparison: Security Design Choices," Microsoft Developer Network October,2002.

[30]. Minaam D S A, Kader H M A, and Hadhoud M M "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types", International Journal of Network Security, Vol.11, No.2, PP.78-87, Sept,2010.

[31]. Uddin M, Khowaja K and Rehman A A "Dynamic Multi-Layer Signature Based Intrusion Detection System Using Mobile Agents", International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.4, October,2010.

[32]. Sen J " An intrusion Detection Architecture for Clustered Wireless Ad Hoc Networks", Second International Conference on Computational Intelligence, Communication Systems and Networks,2010.

[33]. Schneier B "Applied Cryptography", John Wiley and Sons, Inc, 1996.

[34]. Singh B "Network Security and Management" PHI, New Delhi, 2006.

[35]. Stallings W "Cryptography and Network Security, Principles and Practices" Pearson Education, New Delhi ,2005.

[36]. " Rsa-Based Digital Image Encryption Algorithm In Wireless Sensor Networks" Gaochang Zhao, Xiaolin Yang, Bin Zhou, Wei Wei University of Science and Technology, Chengdu 610065

[37]. " A Survey on Wireless Sensor Network Security" Jaydip Sen, Tata Consultancy Services Limited, Wireless & Multimedia Innovation Lab, Bengal Intelligent Park, Salt Lake Electronics Complex, Kolkata 700091, India

[38]. "Network Security Protocols for Wireless Sensor Networks-A Survey" Pritam Gajkumar Shah Lecturer, Telecom Engineering Department RV College of Engineering, Bangalore

[39]. Fei Hu "Secure Wireless Sensor Networks: Problems and Solutions", IEEE Senior Member, Electrical & Computer Engineering Department, Clarkson University, Potsdam, New York 13699, USA