APPROACH TO SECURITY IN WIRELESS SENSOR NETWORKS

Himanshu Monga [1], Silki Baghla [2]

[1]Professor, Jan Nayak Chaudhary Devi Lal Vidyapeeth, Sirsa (Haryana)
[2] Assist. Professor, Jan Nayak Chaudhary Devi Lal Vidyapeeth

Abstract:
The future developments of the wireless sensor networks and its applications demands for the efficient and secure communication. For the solution of efficient and reliable security needs cryptography algorithms provides good solutions. For providing reliable security schemes mainly data confidentiality now-a-days key management is used. This paper provides a review over cryptography schemes being used to deal with security issues of wireless sensor networks.

ARTICLE HISTORY
Received 15 August 2016
Accepted 27 August 2016
Available online 30 September 2016

KEYWORDS
Wireless Sensor Networks (WSNs), Efficient and Reliable Security , cryptography, communication, data confidentiality

1. INTRODUCTION

The first section of this paper provides the introductory concepts of WSN, security issues and requirements. The section 2 reviews the cryptographic techniques. In section 3, the reviews for asymmetrical cryptography with key management ideas. Section 4 contains the current and future work in asymmetrical cryptography and finally this paper is concluded with section 5.

1.1 Wireless sensor networks

A wireless sensor node contains components like storage, processing, sensing and transmission as their main electronic components [1]. The computational power possessed by these electronic components is generally low, but these electronic devices are the main play contributors for computing. The task of these electronic devices is to collect data in a wireless network and pass the collected data by the network between the connecting nodes which work as collective unit [2]. The WSNs are applicable for monitoring human body organs, environmental monitoring, temperature and humidity controlling, vehicle traffic controlling systems (Adhoc), etc. (figure 1) shows the basic scenario of wireless sensor networks application in which a basic network is used to monitor the type of an application whether human body organ monitoring, Adhoc network, temperature control or any other application by using sensor nodes for proving the desired computational demands.

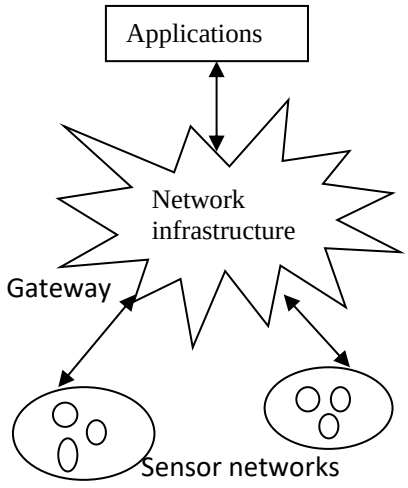

Fig. 1. Wireless sensor network

During communicating through the network a case arises of failure, which is solved by the use self-configuration and adaptation features of WSNs. With the growth of WSNs now there are mostly no monitoring stations in the networks to monitor nodes working during the working life of the network it is being done by sensor nodes by itself [3].

CONTACT: Himanshu Monga, himanshumonga@gmail.com

1.2 Security vulnerabilities

In a WSNs the sensor nodes are deployed not in a confined area but they are spread over a large area, thus their single controlling and monitoring in a network is mostly a not so easy to do task thus allowing the unauthorized users to provides faults and errors in interviewing the security of these sensor nodes without having any physical access to the sensor nodes [4].

WSNs can be divided into three main types:

1. Authentication and Confidentiality attack: By attacking on these security parameters changes are done like repetition or modification of packets.
2. Availability network Attack/DoS attacks/or Negation of service: By such attacks the networks seems to be unavailable for use instead of being actually free to use.
3. Attack on integrity: By integrity attacks the false data packets are continuously communicating between nodes in a network making the network unavailable for communicating useful information and available for attackers to communicate in a network.

1.3 Security requirements

A conventional computer network working is the basic working concept for working of WSNs. Additional requirement is basically security of data communication in WSNs as compared to computer network during a working network life cycle. Security requirements are the additional feature of WSNs which included some certain and important terms such as confidentiality, integrity, availability, authenticity and quality of service.

The security requirements in WSN include [5]:

- confidentiality: An unauthorized user in a network is not allowed to access information in a network;
- authentication: A secret authentication code called MAC is shared between the nodes communicating in a network to achieve secure data communication in a network, providing reliable communication of data form origin to destination;
- integrity: An unauthorized user in a communicating network is not permissioned to transform the information being transferred in a network;
- availability: In WSNs certain services are needed on demand and certain are fixed like node connectivity is sometimes fixed service or is on demand service to provide such services and demands needs in a network at any time availability parameter in a network is used; and,
- quality of Service: In a WSNs security also deals with timely and accurate data packet delivery to avoid data loss.

2. CRYPTOGRAPHY TECHNIQUES

To avoid above explained attacks and to achieve security of data in WSNs mostly cryptographic techniques are being used as an important part of the WSNs security architecture. Cryptography techniques are basically encryption techniques used to encrypt our basic data packets into some secured data packets of coded data words that are being transferred over the network instead of direct original data packets transmission. During transmission encrypted data is basically a set of some extra bits along with the data bits for securing the original data from being accessed by the attackers which is secured and compatible to the existing protocols over the network operating as a layered model of network. Cryptography schemes are provided to meet the basic security requirements of confidentiality and integrity in networks basically there are 2 cryptography algorithms Symmetric Cryptography (secret key) and Asymmetrical Cryptography (public key) [6].

2.1 Symmetrical cryptography - Symmetric encryption/ secret-key cryptography

Preferred system uses a single secret key for both encryption and decryption of the data packets in a communicating network which is kept as secret in a network as shown in (figure 2). The further classification of Symmetric key algorithms is i) block ciphers for fixed transformations, and ii) stream ciphers for time varying transformations.

These 2 subdivisions are used to compare encryption algorithms on plain texts at various levels for example, various data types, battery power consumption parameters, various data block sizes, for various key sizes [14,15] and various encryption/decryption speeds [7,8].

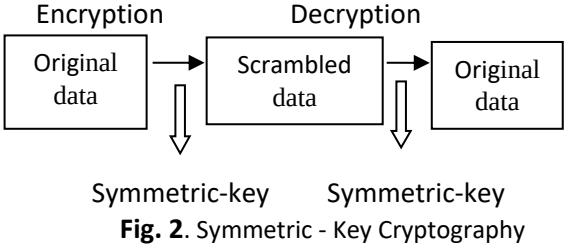

Fig. 2. Symmetric - Key Cryptography

Keeping the key secreted in the network in the most difficult task in the network [9]. Some examples of Symmetric key cryptosystems are AES, DES, RC4 CAST, RC5 algorithms used in WSN [12,13,14,15].

2.2 Asymmetric Cryptography. Asymmetric encryption /public-key cryptography

Presented being used widely cryptography technique is asymmetrical cryptography uses two keys public and private keys for data encryption and decryption which avoids the treat of key sharing in a network to implement reliable security needs [9] as shown in (figure 3).

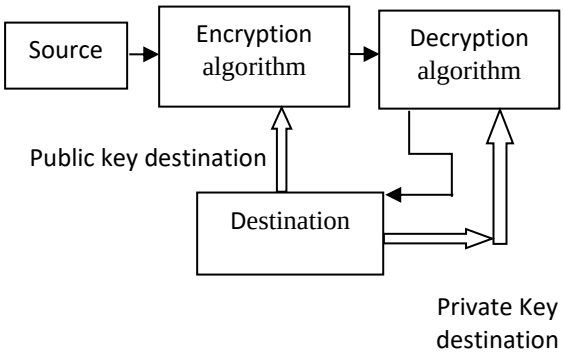

Fig. 3. Asymmetric Key Cryptography

The keys are used as 2 way security providers as private key never makes the encrypted data publically known to every user it is only provided to the authorized users for accessing the data and by having matched private key a user can decrypt the data at the destination end comparing its public and private key with the sender's public and private key.

3. ASYMMETRICAL CRYPTOGRAPHY

A public key cryptography - Asymmetrical Cryptography is basically used now as implemented cryptography technique as it avoids treats of security more efficiently then symmetrical ones. As the basic principle of public key says it consists of a pair of related and different keys i) public: provided publically ii) private: user specified. The keys are related to each other but computationally different also we cannot determine our private key using our public key [10] as shown in (figure 4) thus higher level attacks are avoided using such cryptography algorithms and reduces security complexities also by avoiding known key in a network therefore, mostly applicable in the general public for data communication [11]. Asymmetric public key cryptosystems such as the Diffie-Hellman key agreement [14,15], ECC or RSA signatures are typically usable in WSNs [12].

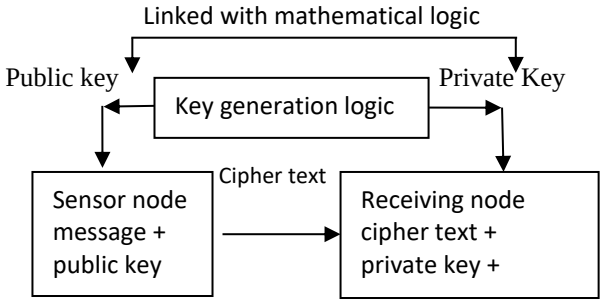

Fig. 4. Public key cryptography

4. CURRENT AND FUTURE WORK

In WSNs Symmetrical cryptography are more prone to security issues while the stronger asymmetrical cryptography still seems to be applicable. The PKC are used presently for solving security issues of WSNs currently mostly ECC, RSA, LPKC (large size PKC), MQ-PKC (multivariate quadratic PKC) [12,13,14,15] are used along with key generation techniques either using static key generation or by using group key generation providing number of WSNs applications successful implementations [14,15].

4.1 Key management schemes

Some major key management schemes used for reliable and efficient security of data by the help of cryptography are listed as:

- network wide shared key [12]: The simplest method for key distribution in which before communicating in a network, a single well known key called network wide shared key which is known and same for all nodes in a network is generated, then this key is used for communicating with all neighbouring nodes providing integrity by using a message authentication code (MAC). The disadvantage of this key is: An unauthorized user can attack and possesses the data being communicating in a network by capturing a single node of the network wide shared key;
- master key and link [13] key: This scheme provides a key named as master key before communicating to all the nodes working in a network and also contains link keys of the communicating codes. Its disadvantages are new nodes addition is a complex task as the network is restricted to single node

compromise attack and also the link keys are not secure during transmitting the data over or between networks;

- public key cryptography: Uses 2 key generation scheme i.e. public and private key generation during encryption of data solving key management and key distribution problems [11]. Its disadvantage is less memory and processing power limitations;
- symmetric keys: In this [10] scheme every node of the communicating network in advance have a set of link keys for establishing secure links with other communicating and neighboring sensor nodes. Its disadvantage is that its non-scalability because every node in a network has to store n (n - 1)/2 keys, for n is the number of nodes in the network; and,
- bootstrapping keys: This [14] scheme is an on-demand key generation scheme for providing secure connections among the communicating sensor nodes. Its disadvantage is suffering of nodes from single point of failure. This failure is due to the base station which has to maintain a database for the link keys of the senor nodes communicating in a network.

4.2 Work being done

The study of these key management schemes are based on the review of some research papers defining some works done on cryptography for solving security issues on data transmission over the network:

- analysis of cryptography for wireless sensor network security by F. Amin, A. H. Jahangir, and H. Rasifard (2008): According to their study RSA is not an efficient technique for data encryption in WSNs. For this they have Compared ECC-160 and RSA-1024. Results shows that implementation of RSA cryptography consumes more efforts for implementing security requirements as compared to ECC-224 which provides more feasible, time and power consumption solutions;
- data security using public key cryptography in WSNs by Amin Reza Sedghi, Mohammad Reza Kaghazgaran (June 2013): The use of public-key cryptography on small wireless devices is provided solving for reliable and efficient authentication and key exchange protocols requirements;
- PKC-Based DoS Attacks-Resistant Scheme in Wireless Sensor Networks by Daehee Kim, Sunshin An (April 15, 2016): PKC-based cryptography resistance schemes are good to avoid DoS attacks and are energy-efficient and always keeps data packets under accepted capacity limits even if large number of false packets are being generated by neighbouring cells;
- Public-Key Cryptographic Primitives in Wireless Sensor Networks by Kyung-Ah Shim (2016): For data communication and transmission PKC primitives are efficient solution providers in making decisions and designing security schemes on WSN networks which are directly applicable for WSNs applications without much modification; and,
- key generations from wireless channels by Junqing Zhang, Trung q. Duong, Alan Marshall, and Roger woods (2016): For easy and efficient practical working of key generation with cryptography algorithms in WSNs random key generation for wireless communication channels are used.

5. CONCLUSION

Thus concluded information suggests that the symmetrical cryptography is not well suited for WSNs as compared to asymmetrical cryptography. In addition to key management and security, public-key cryptography can be the efficient and reliable scheme for number of WSNs applications. Public key cryptography provides more advantages because of its low memory usage, low CPU consumption, and shorter key size over symmetrical schemes providing positive energy profits than doing random drops. The asymmetrical algorithms are more reliable with variable key management generation techniques providing efficient security goals as the key size is identical and varied at each step without being in need to make them known to all nodes in a network as private key is not computed by public key of the network provided as a security feature of asymmetrical cryptosystems. Also the asymmetrical cryptosystems are more efficient in security goals achievement as compared to symmetrical ones as they need to provide the link keys publically which causes unauthorized attacks and user's data security defects.

REFERENCES

[1] K. Akkaya, M. Younis, A Survey of Routing Protocols in Wireless Sensor Networks, Elsevier Ad Hoc Network Journal, 3 (3), 2005: 325-349. doi:10.1016/j.adhoc.2003.09.010

[2] S.G. Quirino, A.R.L. Riberio E.D. Moreno, Asymmetrical encryption in wireless sensor networks, 2012, 217-232.

[3] E. Shi, A. Perrig, Designing secure sensor networks, Wireless communication magazine, 11 (6), 2004: 37-43.

[4] Y. Wang, G. Attebeery, B. Ramamurthy, A Survey of security issues in wireless sensor networks, IEEE communication surveys and tutorials, 8 (2), 2006: 2-23.

[5] Y. Wang, W. Gee, S. Chellappan, D. Xuan, Ten H. Laii, Search-based physical attacks in sensor networks: Modeling and Defense, technical report, Department of computer science and engineering, Ohio State University, 2005.

[6] S. Ahmad, M.R. Beg, Q. Abbas, Energy saving secure framework for sensor network using elliptical curve cryptography, Mobile Adhoc networks, 2010: 167-172.

[7] R. Ahlswede, I. Csiszar, Common in information theory and cryptography I. secret sharing, IEEE Transactions on Information Theory, 39 (4), 1993: 1121-1132.

[8] D.H. Kerson, A. Meneres, S. Vanstone, Guide to Elliptical curve cryptography, Springer-Verlag New York, Inc. 2004.

[9] A.J. Menezes, P.C. Van Oorschot, S.A. Vanstone, Handbook of applied cryptography, CRC Press, 1996.

[10] G. Gaubtaz, J.P. Kaps, B. Sunar, Public key in sensor networks-revisited, 133, 2004: 2-18.

[11] A. S. Wander, N. Gura, H. Eberle, V. Gupta S. C. Shantz, Energy analysis of public key cryptography for wireless sensor network, 3rd IEEE Conference on Pervasive Computing and Communications, 2005: 324-328.

[12] Y. Zhang, The Scheme of public key infrastructure for improving wireless sensor networks security, Software Engineering and Service Science (ICSESS), 2012 IEEE 3rd International Conference, 22-24 June, 2012, pp.527-530.

[13] W. D., J. Deny, Y. S. Han, S. Chen, P. K. Varshney, A key management scheme for wireless sensor network using deployment knowledge, 2004.

[14] O. Gungor, F. Chen, C.E. Koksal, Secrete key generation via localization and mobility, IEEE Transactions on Vehicular Technology, 6 (6) 2015: 2214-2230.

[15] H. Liu, J. Yang, Y. Wang, Y.J. Chen, C.E. Koksal, Group secret key generation via received signal strength: Protocols, achievable rates, and implementation, IEEE Transactions on Mobile Computing, 13 (12), 2014: 2820-2835.