Scientific Journal of Impact Factor(SJIF): 3.134
e-ISSN(O): 2348-4470
p-ISSN(P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 2,Issue 10, October-2015

A Survey on Cryptographic Approaches to provide privacy preservation in Wireless Sensor Networks

Bannishikha Banerjee[1], Jalpa T. Patel [2]

[1]Sri S'ad Vidya Mandal Institute of Technology CS – IT, Gujarat Technological University
[2]Sri S'ad Vidya Mandal Institute of Technology CS – IT, Gujarat Technological University

Abstract – *A wireless sensor network (WSN) consists of spatially distributed independent autonomous sensors that monitor physical or environmental conditions, such as temperature, sound, pressure, etc. They cooperate with each other and pass their sensor activity information to each other. The development of wireless sensor networks was inspired by military applications like battlefield surveillance, etc. Today such networks are being used in many industrial and consumer applications, like industrial process monitoring and control, machine health monitoring, and so on. Many algorithms are already developed for obtaining security and privacy preservation in wireless sensor network but they have many limitations. Wireless Sensor Networks (WSN) has many advantages in real-world applications, but it is also prone to various vulnerabilities. The threats faced by these networks are similar but are not limited to the threats seen in simple network of computers or Internet. Due to vulnerabilities on WSNs the malicious attacker node can access sensitive information that is transferred among the sensor nodes without encryption. One way to avoid this is to encrypt the data being transferred from source to destination. This provides privacy because malicious users cannot read encrypted data. There are many already designed and tested encryption algorithms to achieve this. In this paper, we have surveyed and compared some of those encryption algorithms.*

Keywords *– Wireless Sensor Network, Encryption, Decryption, Symmetric Key, Cryptography.*

I. INTRODUCTION

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their control of sensor activity [1]. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. But wireless sensor networks are vulnerable to many attacks and threats. Many algorithms are already developed for security in wireless sensor network but with many limitations. The attacks on WSN prove to be even more destructive than those on internet or other ad hoc networks [1].

The reason is the WSN consists of nodes with very limited resources whereas the attacker may have very powerful attacking (malicious) resources such as laptops with wireless LAN capability, long range wireless communication capability etc. Therefore security in WSN is a major issue.

The security techniques of the normal computer networks cannot be implemented in WSN because of limited resources. Considering, for example, the asymmetric cryptographic algorithm like RSA cannot be used for encryption because the memory of a typical sensor node is not sufficient enough to hold even the variables for its implementation. Even if memory is allowed the computation time would be enormous.

To worsen the situation the power available with a sensor node is also very small and the node may even entirely consume its energy in a single computation. So we understand that the normal computationally heavy algorithms of security can't be applied on WSN which has limited resources.

Therefore, we need light weight cryptographic algorithms to provide encryption and decryption of information in WSN [1]. In this paper we surveyed and compared symmetric algorithms because asymmetric algorithms are not feasible to implement in WSN. Symmetric algorithms provide encryption and decryption using the same key.

II. SECURITY ISSUES IN WSN

The wireless nature of the WSN and its resources limitations make them vulnerable to several types of attacks. Such attacks can be carried out in a variety of ways; common types of attacks are the denial of service attacks (DoS), traffic analysis attacks, eavesdropping, physical attacks, etc [1].

Spoofed, Altered, or Replayed Routing Information – By spoofing, altering, or replaying routing information, the adversaries could potentially create routing loops, attract or repel network traffic, lengthen or shorten routes, generate fake error messages, partition the network, increase node to node latency[2].

Selective Forwarding Attack – Malicious nodes could prevent forwarding certain messages or even discard them; consequently, these messages would not propagate through the network [2].

Sinkhole Attack – The goal of the adversary is to attract all the traffic to a certain area or the network through a compromised node, creating a sinkhole [2].

HELLO Flood Attack – Some protocols require nodes to send HELLO packets to advertise themselves to their neighbors. If a node receives such packet, it would assume that it is inside the RF range of the node that sent that

packet. However, this assumption could be false because a laptop class adversary could easily send these packets with enough power to convince all the network nodes that the adversary is their neighbor. But the transmission power of those nodes is much less that the adversary's, thus the packets would get lost, and that would create a state of confusion in the sensor network [2].

III. SECURITY REQUIREMENTS

Confidentiality - Confidentiality ensures the concealment of the message from an attacker so that any message communicated via the sensor network remains confidential [3].

Authentication - Authentication ensures the reliability of the message by identifying its origin. By authenticating other nodes, cluster heads, and base stations before granting a limited resource, or revealing information [3].

Integrity - Integrity ensures the reliability of the data and refers to the ability to confirm that a message has not been tampered with, altered or changed while on the network [3].

Availability - Availability ensures the services of resources offered by the network, or by a single sensor node must be available whenever required [3].

IV. RELATED WORK

In [7] LEE is a 64-bit block Feistel Network with a 128-bit key and a suggested 32 rounds. The Feistel Function is based on fixed length rotation and shift operations, XOR and addition modulo 2^{32}. In LEE, as in other Feistel type of ciphers, the plain text block is split into two halves, L_0 and R_0. Each half is used to encrypt the other half over 32 rounds of processing and then combine to produce the cipher text block. Therefore, the original input of the algorithm (i.e. plain text) is $P = L_0.R_0$ and the final cipher text is $C = L_{32}.R_{32}$.

In [8] TEA (Tiny Encryption Algorithm) and its related variants (XTEA, Block TEA, XXTEA) are symmetric key block ciphers designed for modern 32-bit word architecture. The emphasis of TEA is on small code size and easy implementation with typically few lines of codes. It uses a large number of iterations rather than a complicated algorithm. All TEA and its variants are based on the Feistel structure, every TEA cycle consists of two Feistel rounds. TEA and XTEA operate on two 32-bit words as a 64-bit data blocks with a 128-bit key, therefore all operations are done in 32-bit words. Block TEA and XXTEA operate on variable-length blocks of arbitrary multiples of 32 bits size. The advantage of Block and XXTEA is that it eliminates the need for using a mode of operation (CBC, OFB, CFB, OCB etc.) on messages larger than one block. i.e., they can be applied directly to a complete message.

In [8] TREYFER is a 64-bit block cipher with 64-bit symmetric key. It is aimed at applications with extremely limited resources, e.g. smart card and is designed to be very compact (less than 50 bytes of code on an 8051 microcontroller with assembler language). It can be executed on a very constrained architecture, for example an 8051 microcontroller with typically 1 KB flash EPROM, 64 bytes RAM, 128 bytes EPROM and a peak instruction rate of 1 MHz. TREYFER is designed to use only byte operations and requires fixed bit rotations and modulo 256 additions.

In [8] RC5 is a symmetric encryption algorithm with a block size of 32, 64, or 128 bits. The key length ranges from 0 to 2040 bits. RC5 encrypts two-word blocks, for example a 32-bit block has a word size of 16-bit. The maximum number of RC5 rounds is 255, but typically 12 rounds encryption/decryption algorithm is suggested. RC5 has a simple structure similar to a Feistel structure. Instead of half of a block being updated as in the classic Feistel structure, both halves are updated in each RC5 round [6]. RC5 uses only three primitive operations: modulo 2n addition or subtraction (n is the word size), XOR, and circular rotation. The encryption/decryption algorithm is very simple and can be implemented in few lines of codes. These characteristics make RC5 suitable for both hardware and software implementations.

In [10] AES algorithm is a symmetric block cipher that processes data blocks of 128 bits using a cipher key of length 128, 192, or 256 bits. Each data block consists of a 4×4 array of bytes called the state, on which the basic operations of the AES algorithm are performed.

The proposed algorithm in [10] differs from conventional AES as it has 200 bits block size and key size both. Number of rounds is constant and equal to ten in this algorithm. The key expansion and substitution box generation are done in the same way as in conventional AES block cipher. AES has 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.

In [11] Blowfish is a 64-bit block cipher with a variable length key. It defines 2 distinct boxes: S boxes, a P box and four S boxes. Taking into consideration the P box P is a one-dimensional field with 18 32-bit values. The boxes contain variable values; those can be implemented in the code or generated during each initialization. The S boxes S1, S2, S3, and S4 each contain 256 32-bit values.

In [12] the modified DES encrypts 64-bit blocks with a 56 bit key K. after an initial permutation of the bits, a plaintext block goes through 16 iterations (rounds) of a complex function and then passes through a final permutation that yields the cipher text block. During each round i, the right half of the block is expanded to 48 bits and XORed with a 48 bit internal key Ki derived from K. the result then passes through 6 s-boxes which are nonlinear substitutions results 32 output bits from 8 input bits.

V. COMPARATIVE ANALYSIS [19]

Sr. No.	Algorithm	Block Size (Bits)	Key Size (Bits)	Evaluation
1.	DES	64	56	Insecure block cipher [6]
2.	AES	128	256	Better than DES
3.	Blowfish	64	32-448 (128 by default)	Better than all other algorithms [14]
4.	RC5	32,64 or 128 bits	0-2040 bits	Simple and easy to implement
5.	TEA	64 bits	128 bits	Small sized
6.	TREYFER	64 bits	64 bits	Very compact
7.	LEE	64 bits	128 bits	Very fast and light weight

Table 1 Comparative Analysis

VI. CONCLUSION

After studying various algorithms we conclude that, Blowfish and LEE are the best encryption algorithms for providing confidentiality in wireless sensor networks. These are light weight and are feasible to implement. Wireless sensor networks have limited resources, so it is important that the encryption algorithms are light weight. Blowfish and LEE have smaller block size and key size. These two are easy to implement. Blowfish and LEE provide better security in wireless sensor networks. Therefore, these two are more efficient cryptographic algorithms in wireless sensor networks [7].

REFERENCES

[1] Pinak M. Popat, Pooja A. Vaishnav, Ankita M. Parmar, Bhumi K. Padodara, “CRYPTOGRAPHIC ALGORITHMS FOR WIRELESS SENSOR NETWORK”, JIKRCE, VOLUME – 02, ISSUE – 02, 2013.
[2] Virendra Pal Singh, Aishwarya S. Anand Ukey, Sweta Jain, “Signal Strength based Hello Flood Attack Detection and Prevention in Wireless Sensor Networks”, IJCA, Volume 62– No.15, January 2013.
[3] Gaurav Sharma, Suman Bala, Anil K. Verma, “Security Frameworks for Wireless Sensor Networks-Review”, Elsevier, ICCCS-2012.
[4] Xiong, X., Wong, D., Deng, “TinyPairing: A Fast and Lightweight Pairing-based Cryptographic Library for Wireless Sensor Networks”, WCNC 2010, IEEE Communications Society.
[5] Supratim Saha, “Low Power AES Algorithm Implementation for Wireless Communication”, International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 2 Issue 8, August - 2013. pp. 29-31. Alan Kaminsky.
[6] Cai-hong Liua, Jin-shui Jia, Zi-long Liua, "Implementation of DES Encryption Arithmetic based on FPGA", Elsevier, AASRI Procedia 5, 2013, pp. 209 – 213.
[7] Nikos Komninos, Hamed Soroush, and Mastooreh Salajegheh, “LEE: Light-Weight Energy-Efficient Encryption Algorithm for Sensor Networks”, IEEE conference, 9th International Symposium on Communication Theory & Applications (ISCTA’07), IEEE 2007.
[8] Soufiene Ben Othman, Abdelbasset Trad, Habib Youssef, “Performance Evaluation Of Encryption Algorithm For Wireless Sensor Networks”, IEEE conference, ICITS, 2012.
[9] E. Shi and A. Perrig, “Designing Secure Sensor Networks”, IEEE Wireless Communications Magazine, pp. 38-43, December 2004.
[10] Ritu Pahal, Vikas kumar, “Efficient Implementation of AES, IJARCSSE”, Volume 3, Issue 7, July 2013.
[11] Ms NehaKhatri – Valmik, Prof. V. K Kshirsagar, “Blowfish Algorithm”, IOSR-JCE, Volume 16, Issue 2, 2014.
[12] Prashanti.G, Deepthi.S, Sandhya Rani.K, “A Novel Approach for Data Encryption Standard Algorithm”, IJEAT, Volume-2, Issue-5, June 2013.
[13] Xinmiao Zhang and Keshab K. Parhi, “Implementation approaches for the advanced encryption standard algorithm”, IEEE Conference - 2002.

[14] TingyuanNie; Teng Zhang; , "A study of DES and Blowfish encryption algorithm," TENCON 2009 - 2009 IEEE Region 10 Conference , vol., no., pp.1-4, 23-26 Jan. 2009.
[15] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A Survey on Sensor Networks", IEEE Communications Magazine, pp. 102-114, August 2002.
[16] C. Karlof, D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", Elsevier's Ad Hoc Networks Journal, Special Issue on Sensor Network Applications and protocols, 2003, 1-3.
[17] R. Rivest, "The RC5 Encryption Algorithm", Proceedings of the 7th Annual International Conference on Mobile Computing and Networking, 1995, Springer-Verlag, 86-96.
[18] R. Venugopalan, P. Ganesan, P. Peddabachagari, A. Dean, F. Mueller, M. Sichitiu, "Encryption overhead in embedded systems and sensor network nodes: Modeling and analysis", International Conference on Compilers, Architectures and Synthesis for Embedded Systems, 2003.
[19] Rishab Arora, Sandeep Sharma, PhD "Performance Analysis of Cryptography algorithms", International Journal of Computer Applications (0975 – 8887) Volume 48 No.21, June 2012 ,pp.35-39.
[20] Mayur K. Joshi, Asst.Prof. Haresh Rathod, "State of Art: Survey of Cryptographic Algorithm in Wireless Sensor Networks", IJSRD, Vol. 2, Issue 11, 2015.
[21] X. Zhang, H.M. Heys, and C. Li, "An Analysis of Link Layer Encryption Schemes in Wireless Sensor Networks," in Proc of IEEE International Conference on Communications (ICC 2010), p.168-172, May 2010.
[22]Y. W. Law, J. M. Doumen, and P. H. Hartel. "Benchmarking block ciphers for wireless sensor networks (extended abstract)". In 1st IEEE Int. Conf. on Mobile Adhoc and Sensor Systems (MASS), Oct 2004. IEEE.
[23] C. Karlof, D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", Elsevier's Ad Hoc Networks Journal, Special Issue on Sensor Network Applications and protocols, p.1-32003.
[24] B. Preneel, V. Rijmen, "Cryptographic primitives for information authentication - state of the art", State of the Art in Applied Cryptography,1998.
[25] R. Venugopalan, P. Ganesan, P. Peddabachagari, A. Dean, F. Mueller, M. Sichitiu, "Encryption overhead in embedded systems and sensor network nodes: Modeling and analysis", International Conference on Compilers, Architectures and Synthesis for Embedded Systems, 2003.

